

I hereby certify that this correspondence is being deposited with the U.S. Postal Service with sufficient postage as First Class Mail, in an envelope addressed to: Commissioner for Patents, Washington, DC 20231, on the date shown below.

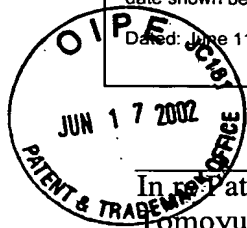
Dated: June 11, 2002

Signature:

Robert B. Cohen
(Robert B. Cohen)

#7

Docket No.: SONYJP 3.0-239
(PATENT)



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Patent Application of:
Tomoyuki Asano

Application No.: 10/075,016

Group Art Unit: 2131

Filed: February 13, 2002

Examiner: Not Yet Assigned

For: INFORMATION PLAYBACK DEVICE,
INFORMATION RECORDING DEVICE,
INFORMATION PLAYBACK METHOD,
INFORMATION RECORDING METHOD,
AND INFORMATION RECORDING MEDIUM
AND PROGRAM STORAGE MEDIUM USED
THEREWITH

CLAIM FOR PRIORITY AND SUBMISSION OF DOCUMENTS

Commissioner for Patents
Washington, DC 20231

Dear Sir:

Applicant hereby claims priority under 35 U.S.C. 119 based on the following
prior foreign application filed in the following foreign country on the date indicated:

<u>Country</u>	<u>Application No.</u>	<u>Date</u>
Japan	JP2001-034969	February 13, 2001

In support of this claim, a certified copy of the original foreign application is filed
herewith.

Dated: June 11, 2002

Respectfully submitted,

By

Robert B. Cohen

Robert B. Cohen

Registration No.: 32,768

LERNER, DAVID, LITTENBERG,
KRUMHOLZ & MENTLIK, LLP
600 South Avenue West
Westfield, New Jersey 07090
(908) 654-5000
Attorneys for Applicant

S02P01830500



日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2001年 2月13日

出 願 番 号

Application Number:

特願2001-034969

[ST.10/C]:

[JP2001-034969]

出 願 人

Applicant(s):

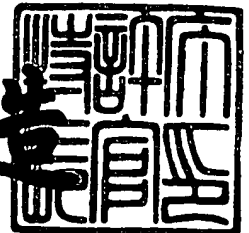
ソニー株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2002年 1月11日

特 許 庁 長 官
Commissioner,
Japan Patent Office

及 川 耕 造



【書類名】 特許願

【整理番号】 0000611207

【提出日】 平成13年 2月13日

【あて先】 特許庁長官殿

【国際特許分類】 G09C 1/00

【発明者】

 【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

 【氏名】 浅野 智之

【特許出願人】

 【識別番号】 000002185

 【氏名又は名称】 ソニー株式会社

 【代表者】 出井 伸之

【代理人】

 【識別番号】 100101801

 【弁理士】

 【氏名又は名称】 山田 英治

 【電話番号】 03-5541-7577

【選任した代理人】

 【識別番号】 100093241

 【弁理士】

 【氏名又は名称】 宮田 正昭

 【電話番号】 03-5541-7577

【選任した代理人】

 【識別番号】 100086531

 【弁理士】

 【氏名又は名称】 澤田 俊夫

 【電話番号】 03-5541-7577

【手数料の表示】

【予納台帳番号】 062721

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9904833

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報再生装置、情報記録装置、情報再生方法、情報記録方法、および情報記録媒体、並びにプログラム記憶媒体

【特許請求の範囲】

【請求項 1】

記録媒体から情報を再生する情報再生装置において、

前記記録媒体に格納された暗号化コンテンツ記録主体の公開鍵証明書の検証処理を実行し、正当性の確認された公開鍵証明書から前記コンテンツ記録主体の公開鍵を取得して、該取得した公開鍵に基づいて、コンテンツ記録主体のデジタル署名の検証処理を実行し、該検証の結果、署名の正当性が確認されたことを条件として暗号化コンテンツの復号処理を実行することを特徴とする情報再生装置。

【請求項 2】

前記暗号処理手段は、

前記記録媒体に格納された暗号化コンテンツのコンテンツを署名対象として生成されたコンテンツ記録主体のデジタル署名の検証処理を実行し、該検証の結果、署名の正当性が確認されたことを条件として暗号化コンテンツの復号処理を実行する構成であることを特徴とする請求項 1 に記載の情報再生装置。

【請求項 3】

前記暗号処理手段は、

前記記録媒体に格納された暗号化コンテンツに対応して設定されるタイトルキーを署名対象として生成されたコンテンツ記録主体のデジタル署名の検証処理を実行し、該検証の結果、署名の正当性が確認されたことを条件として暗号化コンテンツの復号処理を実行する構成であることを特徴とする請求項 1 に記載の情報再生装置。

【請求項 4】

前記情報再生装置は、

複数の異なる情報再生装置をリーフとした階層キーツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーとを保有し、

前記暗号処理手段は、

前記情報再生装置に内蔵したキーに基づいてキーツリーのパス上の下位キーによる上位キーの暗号化処理データからなる有効化キーブロック（EKB）の復号を実行して前記記録媒体に格納された暗号データの復号処理に必要な復号キー生成データを取得する構成を有することを特徴とする請求項 1 に記載の情報再生装置。

【請求項 5】

前記復号キー生成データは、複数の情報再生装置において共通なマスターキー、または記録媒体に固有のメディアキーであることを特徴とする請求項 4 に記載の情報再生装置。

【請求項 6】

記録媒体に対して情報を記録する情報記録装置において、
記録媒体に格納するコンテンツの暗号化処理を実行する暗号処理手段を有し、
該暗号処理手段は、前記格納コンテンツの記録主体のデジタル署名を生成し、暗号化コンテンツ、デジタル署名および、暗号化コンテンツ記録主体の公開鍵証明書を対応付けて記録媒体に格納する処理を実行する構成を有することを特徴とする情報記録装置。

【請求項 7】

前記情報記録装置は、
格納コンテンツ、デジタル署名、公開鍵証明書のアドレスを対応付けた管理テーブルを生成し、前記記録媒体に格納する処理を実行する構成を有することを特徴とする請求項 6 に記載の情報記録装置。

【請求項 8】

前記暗号処理手段は、
前記記録媒体に格納する暗号化コンテンツのコンテンツを署名対象としてコンテンツ記録主体のデジタル署名の生成処理を実行し、生成した署名を格納コンテンツに対応付けて格納する構成であることを特徴とする請求項 6 に記載の情報記録装置。

【請求項 9】

前記暗号処理手段は、

前記記録媒体に格納する暗号化コンテンツに対応して設定されるタイトルキーを署名対象としてコンテンツ記録主体のデジタル署名の生成処理を実行し、生成した署名を格納コンテンツに対応付けて格納する構成であることを特徴とする請求項6に記載の情報記録装置。

【請求項10】

前記情報記録装置は、

複数の異なる情報記録装置をリーフとした階層キーツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーとを保有し、

前記暗号処理手段は、

前記情報記録装置に内蔵したキーに基づいてキーツリーのパス上の下位キーによる上位キーの暗号化処理データからなる有効化キーブロック（EKB）の復号を実行して前記記録媒体に格納するデータの暗号化処理に必要な暗号化キー生成用データを取得する構成を有することを特徴とする請求項6に記載の情報記録装置。

【請求項11】

前記暗号化キー生成用データは、複数の情報記録装置において共通なマスターキー、または記録媒体に固有のメディアキーであることを特徴とする請求項10に記載の情報記録装置。

【請求項12】

記録媒体から情報を再生する情報再生方法において、

前記記録媒体に格納された暗号化コンテンツ記録主体の公開鍵証明書を検証処理を実行する公開鍵証明書検証ステップと、

正当性の確認された公開鍵証明書から前記コンテンツ記録主体の公開鍵を取得して、該取得した公開鍵に基づいて、コンテンツ記録主体のデジタル署名の検証処理を実行する署名検証ステップと、

該署名検証の結果、署名の正当性が確認されたことを条件として暗号化コンテンツの復号処理を実行するステップと、

を有することを特徴とする情報再生方法。

【請求項13】

前記情報再生方法における前記署名検証ステップは、

前記記録媒体に格納された暗号化コンテンツのコンテンツを署名対象として生成されたコンテンツ記録主体のデジタル署名の検証処理を実行するステップを含み、該検証の結果、署名の正当性が確認されたことを条件として暗号化コンテンツの復号処理を実行することを特徴とする請求項 1 2 に記載の情報再生方法。

【請求項 1 4】

前記情報再生方法における前記署名検証ステップは、

前記記録媒体に格納された暗号化コンテンツに対応して設定されるタイトルキーを署名対象として生成されたコンテンツ記録主体のデジタル署名の検証処理を実行するステップを含み、該検証の結果、署名の正当性が確認されたことを条件として暗号化コンテンツの復号処理を実行することを特徴とする請求項 1 2 に記載の情報再生方法。

【請求項 1 5】

前記情報再生方法は、さらに、

複数の異なる情報再生装置をリーフとした階層キーツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーに基づいて、有効化キーブロック（EKB）の復号を実行して前記記録媒体に格納された暗号データの復号処理に必要な復号キー生成用データを取得する処理を実行することを特徴とする請求項 1 2 に記載の情報再生方法。

【請求項 1 6】

記録媒体に対して情報を記録する情報記録方法において、

記録媒体に格納するコンテンツの暗号化処理を実行する暗号処理ステップと、

前記格納コンテンツの記録主体のデジタル署名を生成するステップと、

暗号化コンテンツ、デジタル署名および、暗号化コンテンツ記録主体の公開鍵証明書に対応付けて記録媒体に格納するステップと、

を有することを特徴とする情報記録方法。

【請求項 1 7】

前記情報記録方法は、さらに、

格納コンテンツ、デジタル署名、公開鍵証明書のアドレスに対応付けた管理テ

ーブルを生成し、前記記録媒体に格納する処理を実行することを特徴とする請求項 1 6 に記載の情報記録方法。

【請求項 1 8】

前記情報記録方法は、さらに、

前記記録媒体に格納する暗号化コンテンツのコンテンツを署名対象としてコンテンツ記録主体のデジタル署名の生成処理を実行し、生成した署名を格納コンテンツに対応付けて格納することを特徴とする請求項 1 6 に記載の情報記録方法。

【請求項 1 9】

前記情報記録方法は、さらに、

前記記録媒体に格納する暗号化コンテンツに対応して設定されるタイトルキーを署名対象としてコンテンツ記録主体のデジタル署名の生成処理を実行し、生成した署名を格納コンテンツに対応付けて格納することを特徴とする請求項 1 6 に記載の情報記録方法。

【請求項 2 0】

前記情報記録方法は、さらに、

前記情報記録装置に内蔵した複数の異なる情報記録装置をリーフとした階層キーツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーに基づいて有効化キーブロック（EKB）の復号を実行して前記記録媒体に格納するデータの暗号化処理に必要な暗号化キー生成用データを取得する処理を実行することを特徴とする請求項 1 6 に記載の情報記録方法。

【請求項 2 1】

暗号化コンテンツを格納した情報記録媒体であり、

該暗号化コンテンツを記録した記録主体の識別データと、

前記記録主体の公開鍵証明書と、

前記記録主体のデジタル署名とを格納したことを特徴とする情報記録媒体。

【請求項 2 2】

前記情報記録媒体は、さらに、

格納コンテンツ、デジタル署名、公開鍵証明書のアドレスを対応付けた管理テーブルを格納したことを特徴とする請求項 2 1 に記載の情報記録媒体。

【請求項 2 3】

記録媒体から情報を再生する情報再生処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを格納したプログラム記憶媒体であって、前記コンピュータ・プログラムは、

前記記録媒体に格納された暗号化コンテンツ記録主体の公開鍵証明書の検証処理を実行する公開鍵証明書検証ステップと、

正当性の確認された公開鍵証明書から前記コンテンツ記録主体の公開鍵を取得して、該取得した公開鍵に基づいて、コンテンツ記録主体のデジタル署名の検証処理を実行する署名検証ステップと、

該署名検証の結果、署名の正当性が確認されたことを条件として暗号化コンテンツの復号処理を実行するステップと、

を有することを特徴とするプログラム記憶媒体。

【請求項 2 4】

記録媒体に対して情報を記録する情報記録処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを格納したプログラム記憶媒体であって、前記コンピュータ・プログラムは、

記録媒体に格納するコンテンツの暗号化処理を実行する暗号処理ステップと、

前記格納コンテンツの記録主体のデジタル署名を生成するステップと、

暗号化コンテンツ、デジタル署名および、暗号化コンテンツ記録主体の公開鍵証明書を対応付けて記録媒体に格納するステップと、

を有することを特徴とするプログラム記憶媒体。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、情報再生装置、情報記録装置、情報再生方法、情報記録方法、および情報記録媒体、並びにプログラム記憶媒体に関し、特に、情報記録装置がデータを情報記録媒体に記録する際に自身のデジタル署名および公開鍵証明書をデータと共に記録し、情報再生装置がデータを読み出す際に上記デジタル署名および公開鍵証明書の正当性を確認し、また情報記録装置がリボークされていないこと

を確認した後にデータを読み出す構成とした情報再生装置、情報記録装置、情報再生方法、情報記録方法、および情報記録媒体、並びにプログラム記憶媒体に関する。

【0002】

【従来の技術】

デジタル信号処理技術の進歩、発展に伴い、近年においては、情報を、デジタル的に記録する記録装置や記録媒体が普及しつつある。このようなデジタル記録装置および記録媒体によれば、例えば画像や音声を劣化させることなく記録、再生を繰り返すことができる。このようにデジタルデータは画質や音質を維持したまま何度もコピーを繰り返し実行することができるため、コピーが違法に行われた記録媒体が市場に流通することになると、音楽、映画等各種コンテンツの著作権者、あるいは正当な販売権者等の利益が害されることになる。昨今では、このようなデジタルデータの不正なコピーを防ぐため、デジタル記録装置および記録媒体に違法なコピーを防止するための様々な仕組み（システム）が導入されている。

【0003】

例えば、MD（ミニディスク）（MDは商標）装置において、違法なコピーを防止する方法として、SCMS (Serial Copy Management System) が採用されている。SCMSは、データ再生側において、オーディオデータとともにSCMS信号をデジタルインタフェース（D I F）から出力し、データ記録側において、再生側からのSCMS信号に基づいて、再生側からのオーディオデータの記録を制御することにより違法なコピーを防止するシステムである。

【0004】

具体的にはSCMS信号は、オーディオデータが、何度もコピーが許容されるコピーフリー（copy free）のデータであるか、1度だけコピーが許されている（copy once allowed）データであるか、またはコピーが禁止されている（copy prohibited）データであるかを表す信号である。データ記録側において、D I Fからオーディオデータを受信すると、そのオーディオデータとともに送信されるSCMS信号を検出する。そして、SCMS信号が、コピーフリー（copy fre

e) となっている場合には、オーディオデータをSCMS信号とともにミニディスクに記録する。また、SCMS信号が、コピーを1度のみ許可 (copy once allowed) となっている場合には、SCMS信号をコピー禁止 (copy prohibited) に変更して、オーディオデータとともに、ミニディスクに記録する。さらに、SCMS信号が、コピー禁止 (copy prohibited) となっている場合には、オーディオデータの記録を行わない。このようなSCMSを使用した制御を行なうことで、ミニディスク装置では、SCMSによって、著作権を有するオーディオデータが、違法にコピーされるのを防止するようになっている。

【0005】

しかしながら、SCMSは上述のようにSCMS信号に基づいて再生側からのオーディオデータの記録を制御する構成をデータを記録する機器自体が有していることが前提であるため、SCMSの制御を実行する構成を持たないミニディスク装置が製造された場合には、対処するのが困難となる。そこで、例えば、DVDプレーヤでは、コンテンツ・スクランブルシステムを採用することにより、著作権を有するデータの違法コピーを防止する構成となっている。

【0006】

コンテンツ・スクランブルシステムでは、DVD-ROM (Read Only Memory) に、ビデオデータやオーディオデータ等が暗号化されて記録されており、その暗号化されたデータを復号するのに用いるキー (復号鍵) が、ライセンスを受けたDVDプレーヤに与えられる。ライセンスは、不正コピーを行わない等の所定の動作規定に従うように設計されたDVDプレーヤに対して与えられる。従って、ライセンスを受けたDVDプレーヤでは、与えられたキーを利用して、DVD-ROMに記録された暗号化データを復号することにより、DVD-ROMから画像や音声を再生することができる。

【0007】

一方、ライセンスを受けていないDVDプレーヤは、暗号化されたデータを復号するためのキーを有していないため、DVD-ROMに記録された暗号化データの復号を行うことができない。このように、コンテンツ・スクランブルシステム構成では、ライセンス時に要求される条件を満たしていないDVDプレーヤは

、デジタルデータを記録したDVD-ROMの再生を行なえないことになり、不正コピーが防止されるようになっている。

【0008】

しかしながら、DVD-ROMで採用されているコンテンツ・スクランブルシステムは、ユーザによるデータの書き込みが不可能な記録媒体（以下、適宜、ROMメディアという）を対象としており、ユーザによるデータの書き込みが可能な記録媒体（以下、適宜、RAMメディアという）への適用については考慮されていない。

【0009】

即ち、ROMメディアに記録されたデータが暗号化されていても、その暗号化されたデータを、そのまま全部、RAMメディアにコピーした場合には、ライセンスを受けた正当な装置で再生可能な、いわゆる海賊版を作成することができてしまう。

【0010】

そこで、本出願人は、先の特許出願、特開平11-224461号公報（特願平10-25310号）において、個々の記録媒体を識別する為の情報（以下、媒体識別情報と記述する）を、他のデータとともに記録媒体に記録し、この媒体識別情報のライセンスを受けた装置であることを条件として、その条件が満たされた場合にのみ記録媒体の媒体識別情報へのアクセスが可能となる構成を提案した。

【0011】

この方法では、記録媒体上のデータは、媒体識別情報とライセンスを受けることにより得られる秘密キー（マスターキー）により暗号化され、ライセンスを受けていない装置が、この暗号化されたデータを読み出したとしても、意味のあるデータを得ることができないようになっている。なお、装置はライセンスを受ける際、不正な複製（違法コピー）ができないように、その動作が規定される。

【0012】

ライセンスを受けていない装置は、媒体識別情報にアクセスできず、また、媒体識別情報は個々の媒体毎に個別の値となっているため、ライセンスを受けてい

ない装置が、記録媒体に記録されている、暗号化されたデータのすべてを新たな記録媒体に複製したとしても、そのようにして作成された記録媒体に記録されたデータは、ライセンスを受けていない装置は勿論、ライセンスを受けた装置においても、正しく復号することができないから、実質的に、違法コピーが防止されることになる。

【0013】

ところで、上記の構成においては、ライセンスを受けた装置において格納されるマスターキーは全機器において共通であるのが一般的である。このように複数の機器に対して共通のマスターキーを格納するのは、1つの機器で記録された媒体を他の機器で再生可能とする（インターオペラビリティを確保する）ために必要な条件であるからである。

【0014】

しかし、この方式においては、攻撃者が1つの機器の攻撃に成功し、マスターキーを取出した場合、全システムにおいて暗号化されて記録されているデータを復号することができてしまい、システム全体が崩壊する。これを防ぐためには、ある機器が攻撃されてマスターキーが露呈したことが発覚した場合、マスターキーを新たなものに更新し、攻撃に屈した機器以外の全機器に新たに更新されたマスターキーを与えることが必要になる。この構成を実現する一番単純な方式としては、個々の機器に固有の鍵（デバイスキー）を与えておき、新たなマスターキーを個々のデバイスキーで暗号化した値を用意し、記録媒体を介して機器に伝送する方式が考えられるが、機器の台数に比例して伝送すべき全メッセージ量が増加するという問題がある。

【0015】

上記問題を解決する構成として、本出願人は、各情報記録再生装置をn分木の各葉（リーフ）に配置した構成の鍵配信方法を用い、記録媒体もしくは通信回線を介して、コンテンツデータの記録媒体への記録もしくは記録媒体からの再生に必要な鍵（マスターキーもしくはメディアキー）を配信し、これを用いて各装置がコンテンツデータの記録、再生を行うようにすることにより、正当な（秘密が露呈していない装置に）対して少ないメッセージ量でマスターキーもしくはメデ

ィアキーを伝送できる構成を、先に提案し、すでに特許出願（特願平2000-105328）している。具体的には、記録媒体への記録もしくは記録媒体からの再生に必要な鍵を生成するために必要となるキー、例えばn分木の各葉（リーフ）を構成するノードに割り当てたノードキーを更新ノードキーとして設定し、更新ノードキーを正当な機器のみが有するリーフキー、ノードキーで復号可能な態様で暗号化処理した情報を含む有効化キープロック（EKB）を各情報記録再生装置に配信し、有効化キープロック（EKB）を受信した各情報記録再生装置のEKB復号処理により、各装置が記録もしくは記録媒体からの再生に必要な鍵を取得可能とした構成である。

【0016】

【発明が解決しようとする課題】

上記の構成においては、秘密が露呈した装置をシステムから排除することは可能であるが、このためにはどの装置の秘密が露呈したかを特定する必要がある。たとえば、ある装置から盗んだ秘密を搭載したクローンデバイスが作られ、ブラックマーケットで販売されていたことが特定できれば、秘密を盗まれた装置が特定され、システムから排除されることになる。

【0017】

ところで、システムに対する攻撃を考えると、上記のようにクローンデバイスが作られて出まわるのではなく、ある情報記録装置を改造して、たとえば本来は暗号化して記録すべきデータを平文で記録するなどの、不正な記録を行わせて、その結果作られた、不正に記録されたデータを含む記録媒体を販売するなどの行為が考えられる。この場合、その記録媒体にデータを不正に記録した装置が特定できれば、それをシステムから排除し、新しいコンテンツデータをその装置では復号させないように配信することが、上記の方法で可能である。

【0018】

本発明は、上述の問題を解決するものであり、情報記録装置がデータを情報記録媒体に記録する際に自身のデジタル署名および公開鍵証明書をデータと共に記録し、情報再生装置がデータを読み出す際に上記デジタル署名および公開鍵証明書の正当性を確認した後にデータを読み出す構成とすることにより、コンテンツ

記録が正当に行われたものであることを条件として再生を可能とするシステムを提供することを目的とする。

【 0 0 1 9 】

【課題を解決するための手段】

本発明の第1の側面は、

記録媒体から情報を再生する情報再生装置において、

前記記録媒体に格納された暗号化コンテンツ記録主体の公開鍵証明書の検証処理を実行し、正当性の確認された公開鍵証明書から前記コンテンツ記録主体の公開鍵を取得して、該取得した公開鍵に基づいて、コンテンツ記録主体のデジタル署名の検証処理を実行し、該検証の結果、署名の正当性が確認されたことを条件として暗号化コンテンツの復号処理を実行することを特徴とする情報再生装置にある。

【 0 0 2 0 】

さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、前記記録媒体に格納された暗号化コンテンツのコンテンツを署名対象として生成されたコンテンツ記録主体のデジタル署名の検証処理を実行し、該検証の結果、署名の正当性が確認されたことを条件として暗号化コンテンツの復号処理を実行する構成であることを特徴とする。

【 0 0 2 1 】

さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、前記記録媒体に格納された暗号化コンテンツに対応して設定されるタイトルキーを署名対象として生成されたコンテンツ記録主体のデジタル署名の検証処理を実行し、該検証の結果、署名の正当性が確認されたことを条件として暗号化コンテンツの復号処理を実行する構成であることを特徴とする。

【 0 0 2 2 】

さらに、本発明の情報再生装置の一実施態様において、前記情報再生装置は、複数の異なる情報再生装置をリーフとした階層キーツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーとを保有し、前記暗号処理手段は、前記情報再生装置に内蔵したキーに基づいてキーツリーのパス上の

下位キーによる上位キーの暗号化処理データからなる有効化キープロック（EKB）の復号を実行して前記記録媒体に格納された暗号データの復号処理に必要な復号キー生成用データを取得する構成を有することを特徴とする。

【0023】

さらに、本発明の情報再生装置の一実施態様において、前記復号キー生成用データは、複数の情報再生装置において共通なマスターキー、または記録媒体に固有のメディアキーであることを特徴とする。

【0024】

さらに、本発明の第2の側面は、
記録媒体に対して情報を記録する情報記録装置において、
記録媒体に格納するコンテンツの暗号化処理を実行する暗号処理手段を有し、
該暗号処理手段は、前記格納コンテンツの記録主体のデジタル署名を生成し、
暗号化コンテンツ、デジタル署名および、暗号化コンテンツ記録主体の公開鍵証明書を対応付けて記録媒体に格納する処理を実行する構成を有することを特徴とする情報記録装置にある。

【0025】

さらに、本発明の情報記録装置の一実施態様において、前記情報記録装置は、
格納コンテンツ、デジタル署名、公開鍵証明書のアドレスを対応付けた管理テーブルを生成し、前記記録媒体に格納する処理を実行する構成を有することを特徴とする。

【0026】

さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、
前記記録媒体に格納する暗号化コンテンツのコンテンツを署名対象としてコンテンツ記録主体のデジタル署名の生成処理を実行し、生成した署名を格納コンテンツに対応付けて格納する構成であることを特徴とする。

【0027】

さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、
前記記録媒体に格納する暗号化コンテンツに対応して設定されるタイトルキーを署名対象としてコンテンツ記録主体のデジタル署名の生成処理を実行し、生成し

た署名を格納コンテンツに対応付けて格納する構成であることを特徴とする。

【 0 0 2 8 】

さらに、本発明の情報記録装置の一実施態様において、前記情報記録装置は、複数の異なる情報記録装置をリーフとした階層キーツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーとを保有し、前記暗号処理手段は、前記情報記録装置に内蔵したキーに基づいてキーツリーのパス上の下位キーによる上位キーの暗号化処理データからなる有効化キーブロック（EKB）の復号を実行して前記記録媒体に格納するデータの暗号化処理に必要な暗号化キー生成用データを取得する構成を有することを特徴とする。

【 0 0 2 9 】

さらに、本発明の情報記録装置の一実施態様において、前記暗号化キー生成用データは、複数の情報記録装置において共通なマスターキー、または記録媒体に固有のメディアキーであることを特徴とする。

【 0 0 3 0 】

さらに、本発明の第3の側面は、

記録媒体から情報を再生する情報再生方法において、

前記記録媒体に格納された暗号化コンテンツ記録主体の公開鍵証明書の検証処理を実行する公開鍵証明書検証ステップと、

正当性の確認された公開鍵証明書から前記コンテンツ記録主体の公開鍵を取得して、該取得した公開鍵に基づいて、コンテンツ記録主体のデジタル署名の検証処理を実行する署名検証ステップと、

該署名検証の結果、署名の正当性が確認されたことを条件として暗号化コンテンツの復号処理を実行するステップと、

を有することを特徴とする情報再生方法にある。

【 0 0 3 1 】

さらに、本発明の情報再生方法の一実施態様において、前記情報再生方法における前記署名検証ステップは、前記記録媒体に格納された暗号化コンテンツのコンテンツを署名対象として生成されたコンテンツ記録主体のデジタル署名の検証処理を実行するステップを含み、該検証の結果、署名の正当性が確認されたこと

を条件として暗号化コンテンツの復号処理を実行することを特徴とする。

【0032】

さらに、本発明の情報再生方法の一実施態様において、前記情報再生方法における前記署名検証ステップは、前記記録媒体に格納された暗号化コンテンツに対応して設定されるタイトルキーを署名対象として生成されたコンテンツ記録主体のデジタル署名の検証処理を実行するステップを含み、該検証の結果、署名の正当性が確認されたことを条件として暗号化コンテンツの復号処理を実行することを特徴とする。

【0033】

さらに、本発明の情報再生方法の一実施態様において、前記情報再生方法は、さらに、複数の異なる情報再生装置をリーフとした階層キーツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーに基づいて、有効化キープロック（EKB）の復号を実行して前記記録媒体に格納された暗号データの復号処理に必要な復号キー生成用データを取得する処理を実行することを特徴とする。

【0034】

さらに、本発明の第4の側面は、
記録媒体に対して情報を記録する情報記録方法において、
記録媒体に格納するコンテンツの暗号化処理を実行する暗号処理ステップと、
前記格納コンテンツの記録主体のデジタル署名を生成するステップと、
暗号化コンテンツ、デジタル署名および、暗号化コンテンツ記録主体の公開鍵証明書を対応付けて記録媒体に格納するステップと、
を有することを特徴とする情報記録方法にある。

【0035】

さらに、本発明の情報記録方法の一実施態様において、前記情報記録方法は、さらに、格納コンテンツ、デジタル署名、公開鍵証明書のアドレスを対応付けた管理テーブルを生成し、前記記録媒体に格納する処理を実行することを特徴とする。

【0036】

さらに、本発明の情報記録方法の一実施態様において、前記情報記録方法は、さらに、前記記録媒体に格納する暗号化コンテンツのコンテンツを署名対象としてコンテンツ記録主体のデジタル署名の生成処理を実行し、生成した署名を格納コンテンツに対応付けて格納することを特徴とする。

【 0 0 3 7 】

さらに、本発明の情報記録方法の一実施態様において、前記情報記録方法は、さらに、前記記録媒体に格納する暗号化コンテンツに対応して設定されるタイトルキーを署名対象としてコンテンツ記録主体のデジタル署名の生成処理を実行し、生成した署名を格納コンテンツに対応付けて格納することを特徴とする。

【 0 0 3 8 】

さらに、本発明の情報記録方法の一実施態様において、前記情報記録方法は、さらに、前記情報記録装置に内蔵した複数の異なる情報記録装置をリーフとした階層キーツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーに基づいて有効化キーブロック（EKB）の復号を実行して前記記録媒体に格納するデータの暗号化処理に必要な暗号化キー生成用データを取得する処理を実行することを特徴とする。

【 0 0 3 9 】

さらに、本発明の第5の側面は、
暗号化コンテンツを格納した情報記録媒体であり、
該暗号化コンテンツを記録した記録主体の識別データと、
前記記録主体の公開鍵証明書と、
前記記録主体のデジタル署名とを格納したことを特徴とする情報記録媒体にある。

【 0 0 4 0 】

さらに、本発明の情報記録媒体の一実施態様において、前記情報記録媒体は、さらに、格納コンテンツ、デジタル署名、公開鍵証明書のアドレスを対応付けた管理テーブルを格納したことを特徴とする。

【 0 0 4 1 】

さらに、本発明の第6の側面は、

記録媒体から情報を再生する情報再生処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを格納したプログラム記憶媒体であって、前記コンピュータ・プログラムは、

前記記録媒体に格納された暗号化コンテンツ記録主体の公開鍵証明書の検証処理を実行する公開鍵証明書検証ステップと、

正当性の確認された公開鍵証明書から前記コンテンツ記録主体の公開鍵を取得して、該取得した公開鍵に基づいて、コンテンツ記録主体のデジタル署名の検証処理を実行する署名検証ステップと、

該署名検証の結果、署名の正当性が確認されたことを条件として暗号化コンテンツの復号処理を実行するステップと、

を有することを特徴とするプログラム記憶媒体にある。

【0042】

さらに、本発明の第7の側面は、

記録媒体に対して情報を記録する情報記録処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを格納したプログラム記憶媒体であって、前記コンピュータ・プログラムは、

記録媒体に格納するコンテンツの暗号化処理を実行する暗号処理ステップと、

前記格納コンテンツの記録主体のデジタル署名を生成するステップと、

暗号化コンテンツ、デジタル署名および、暗号化コンテンツ記録主体の公開鍵証明書を対応付けて記録媒体に格納するステップと、

を有することを特徴とするプログラム記憶媒体にある。

【0043】

【作用】

本発明においては、情報記録装置がデータを情報記録媒体に記録する際に自身のデジタル署名および公開鍵証明書をデータと共に記録するようにした。このことにより、情報を記録する際には、必ず、どの記録装置が記録したかという証拠もデータと共に記録するようにしているので、もし不正に記録されたデータを含む記録媒体が流通したとしても、それをどの記録装置が記録したか特定できるので、システムからの排除が行える。

【 0 0 4 4 】

さらに、情報再生装置がデータを読み出す際に上記デジタル署名および公開鍵証明書の正当性を確認した後にデータを読み出す構成とした。このことにより、不正な記録装置が、不正な記録データに対してデジタル署名を記録しないような攻撃を無力なものにしている。すなわち、記録されたデータに対して有効なデジタル署名がなければ、正当な再生装置はそのデータを再生しないからである。

【 0 0 4 5 】

【発明の実施の形態】

〔システム構成〕

図 1 は、本発明を適用した記録再生装置 1 0 0 の一実施例構成を示すブロック図である。記録再生装置 1 0 0 は、入出力 I / F (Interface) 1 2 0、M P E G (Moving Picture Experts Group) コーデック 1 3 0、A / D、D / A コンバータ 1 4 1 を備えた入出力 I / F (Interface) 1 4 0、暗号処理手段 1 5 0、ROM (Read Only Memory) 1 6 0、C P U (Central Processing Unit) 1 7 0、メモリ 1 8 0、記録媒体 2 0 0 の記録媒体インタフェース (I / F) 1 9 0、さらにトランスポート・ストリーム処理手段 (T S 処理手段) 3 0 0 を有し、これらはバス 1 1 0 によって相互に接続されている。

【 0 0 4 6 】

入出力 I / F 1 2 0 は、外部から供給される画像、音声、プログラム等の各種コンテンツを構成するデジタル信号を受信し、バス 1 1 0 上に出力するとともに、バス 1 1 0 上のデジタル信号を受信し、外部に出力する。M P E G コーデック 1 3 0 は、バス 1 1 0 を介して供給される M P E G 符号化されたデータを、M P E G デコードし、入出力 I / F 1 4 0 に出力するとともに、入出力 I / F 1 4 0 から供給されるデジタル信号を M P E G エンコードしてバス 1 1 0 上に出力する。入出力 I / F 1 4 0 は、A / D、D / A コンバータ 1 4 1 を内蔵している。入出力 I / F 1 4 0 は、外部から供給されるコンテンツとしてのアナログ信号を受信し、A / D、D / A コンバータ 1 4 1 で A / D (Analog Digital) 変換することで、デジタル信号として、M P E G コーデック 1 3 0 に出力するとともに、M P E G コーデック 1 3 0 からのデジタル信号を、A / D、D / A コンバータ 1 4 1

でD/A (Digital Analog)変換することで、アナログ信号として、外部に出力する。

【 0 0 4 7 】

暗号処理手段150は、例えば、1チップのLSI (Large Scale Integrated Curcuit)で構成され、バス110を介して供給されるコンテンツとしてのデジタル信号を暗号化し、または復号し、バス110上に出力する構成を持つ。なお、暗号処理手段150は1チップLSIに限らず、各種のソフトウェアまたはハードウェアを組み合わせた構成によって実現することも可能である。ソフトウェア構成による処理手段としての構成については後段で説明する。

【 0 0 4 8 】

ROM160は、例えば、記録再生装置ごとに固有の、あるいは複数の記録再生装置のグループごとに固有のデバイスキーであるリーフキーと、複数の記録再生装置、あるいは複数のグループに共有のデバイスキーであるノードキーを記憶している。さらに、記録再生装置固有の、公開鍵暗号系の秘密鍵と、公開鍵証明書、さらに、信頼できるセンタの公開鍵を記憶しておく。

【 0 0 4 9 】

ここで、公開鍵証明書は、図2に示すように、その証明書利用者、例えば記録再生装置のIDと、利用者の公開鍵を格納し、その他のデータをメッセージとして信頼できるセンタ（認証局）がデジタル署名を施したデータである。センタのデジタル署名の検証処理を、予め取得済みのセンタの公開鍵を用いて実行して公開鍵証明書の正当性が確認でき、格納された公開鍵を取り出して利用することができる。

【 0 0 5 0 】

CPU170は、メモリ180に記憶されたプログラムを実行することで、MP EGコーデック130や暗号処理手段150等を制御する。メモリ180は、例えば、不揮発性メモリで、CPU170が実行するプログラムや、CPU170の動作上必要なデータを記憶する。記録媒体インタフェース190は、デジタルデータを記録再生可能な記録媒体200を駆動することにより、記録媒体200からデジタルデータを読み出し（再生し）、バス110上に出力するとともに

、バス 110 を介して供給されるデジタルデータを、記録媒体 200 に供給して記録させる。また、プログラムを ROM 160 に、デバイスキー等をメモリ 180 に記憶する構成としてもよい。

【 0 0 5 1 】

記録媒体 200 は、例えば、DVD、CD 等の光ディスク、光磁気ディスク、磁気ディスク、磁気テープ、あるいは RAM 等の半導体メモリ等のデジタルデータの記憶可能な媒体であり、本実施の形態では、記録媒体インタフェース 190 に対して着脱可能な構成であるとする。但し、記録媒体 200 は、記録再生装置 100 に内蔵する構成としてもよい。

【 0 0 5 2 】

トランスポート・ストリーム処理手段 (TS 処理手段) 300 は、後段において図を用いて詳細に説明するが、例えば複数の TV プログラム (コンテンツ) が多重化されたトランスポートストリームから特定のプログラム (コンテンツ) に対応するトランスポートパケットを取り出して、取り出したトランスポートストリームの出現タイミング情報を各パケットとともに記録媒体 200 に格納するためのデータ処理および、記録媒体 200 からの再生処理時の出現タイミング制御処理を行なう。

【 0 0 5 3 】

トランスポートストリームには、各トランスポートパケットの出現タイミング情報としての A T S (Arrival Time Stamp : 着信時刻スタンプ) が設定されており、このタイミングは M P E G 2 システムズで規定されている仮想的なデコーダである T - S T D (Transport stream System Target Decoder) を破綻させないように符号化時に決定され、トランスポートストリームの再生時には、各トランスポートパケットに付加された A T S によって出現タイミングを制御する。トランスポート・ストリーム処理手段 (TS 処理手段) 300 は、これらの制御を実行する。例えば、トランスポートパケットを記録媒体に記録する場合には、各パケットの間隔を詰めたソースパケットとして記録するが、各トランスポートパケットの出現タイミングを併せて記録媒体に保存することにより、再生時に各パケットの出力タイミングを制御することが可能となる。トランスポート・ストリ

ーム処理手段（TS処理手段）300は、DVD等の記録媒体200へのデータ記録時に、各トランスポートパケットの入力タイミングを表すATS（Arrival Time Stamp：着信時刻スタンプ）を付加して記録する。

【0054】

なお、本発明の処理システムにおいて処理されるデータはトランスポートストリームに従ったフォーマット・データに限られるものではない。従ってトランスポートストリーム以外のデータに関する処理を実行する場合は、図1に示すTS処理手段は必ずしも必要とはならない。

【0055】

〔データ記録処理およびデータ再生処理〕

次に、図1の記録再生装置における記録媒体に対するデータ記録処理および記録媒体からのデータ再生処理について、図3および図4のフローチャートを参照して説明する。外部からのデジタル信号のコンテンツを、記録媒体200に記録する場合においては、図3（A）のフローチャートにしたがった記録処理が行われる。即ち、デジタル信号のコンテンツ（デジタルコンテンツ）が、例えば、IEE（Institute of Electrical and Electronics Engineers）1394シリアルバス等を介して、入出力I/F120に供給されると、ステップS11において、入出力I/F120は、供給されるデジタルコンテンツを受信し、バス110を介して、TS処理手段300または、暗号処理手段150に出力する。

【0056】

受信データがトランスポートストリーム処理を必要とする場合は、TS処理手段300においてトランスポート・ストリーム処理が実行される。TS処理手段300は、ステップS12において、トランスポートストリームを構成する各トランスポートパケットにATSを付加したブロックデータを生成して、バス110を介して、暗号処理手段150に出力する。この処理については、さらに後段で詳細に説明する。

【0057】

暗号処理手段150は、ステップS13において、受信したデジタルコンテンツに対する暗号化処理を実行し、その結果得られる暗号化コンテンツを、バス1

10を介して、記録媒体I/F190に出力する。暗号化コンテンツは、記録媒体I/F190を介して記録媒体200に記録(S14)され、記録処理を終了する。

【0058】

なお、IEEE1394シリアルバスを介して接続した装置相互間で、デジタルコンテンツを伝送するときの、デジタルコンテンツを保護するための規格として、本特許出願人であるソニー株式会社を含む5社によって、5CDTCP(Five Company Digital Transmission Content Protection)(以下、適宜、DTCPという)が定められているが、このDTCPでは、コピーフリーでないデジタルコンテンツを装置相互間で伝送する場合、データ伝送に先立って、送信側と受信側が、コピーを制御するためのコピー制御情報を正しく取り扱えるかどうかの認証を相互に行い、その後、送信側において、デジタルコンテンツを暗号化して伝送し、受信側において、その暗号化されたデジタルコンテンツ(暗号化コンテンツ)を復号するようになっている。

【0059】

このDTCPに規格に基づくデータ送受信においては、データ受信側の入出力I/F120は、ステップS11で、IEEE1394シリアルバスを介して暗号化コンテンツを受信し、その暗号化コンテンツを、DTCPに規格に準拠して復号し、平文のコンテンツとして、その後、暗号処理手段150に出力する。

【0060】

DTCPによるデジタルコンテンツの暗号化は、時間変化するキーを生成し、そのキーを用いて行われる。暗号化されたデジタルコンテンツは、その暗号化に用いたキーを含めて、IEEE1394シリアルバス上を伝送され、受信側では、暗号化されたデジタルコンテンツを、そこに含まれるキーを用いて復号する。

【0061】

なお、DTCPによれば、正確には、キーの初期値と、デジタルコンテンツの暗号化に用いるキーの変更タイミングを表すフラグとが、暗号化コンテンツに含まれる。そして、受信側では、その暗号化コンテンツに含まれるキーの初期値を、やはり、その暗号化コンテンツに含まれるフラグのタイミングで変更してい

くことで、暗号化に用いられたキーが生成され、暗号化コンテンツが復号される。但し、ここでは、暗号化コンテンツに、その復号を行うためのキーが含まれていると等価であると考えても差し支えないため、以下では、そのように考えるものとする。ここで、D T C Pについては、例えば、<http://www.dtcp.com>のURL(Uniform Resource Locator)で特定されるWebページにおいて、インフォメーションバージョン(Informational Version)の取得が可能である。

【 0 0 6 2 】

次に、外部からのアナログ信号のコンテンツを、記録媒体 2 0 0 に記録する場合の処理について、図 3 (B) のフローチャートに従って説明する。アナログ信号のコンテンツ(アナログコンテンツ)が、入出力 I / F 1 4 0 に供給されると、入出力 I / F 1 4 0 は、ステップ S 2 1 において、そのアナログコンテンツを受信し、ステップ S 2 2 に進み、内蔵する A / D, D / A コンバータ 1 4 1 で A / D 変換して、デジタル信号のコンテンツ(デジタルコンテンツ)とする。

【 0 0 6 3 】

このデジタルコンテンツは、M P E G コーデック 1 3 0 に供給され、ステップ S 2 3 において、M P E G エンコード、すなわち M P E G 圧縮による符号化処理が実行され、バス 1 1 0 を介して、暗号処理手段 1 5 0 に供給される。

【 0 0 6 4 】

以下、ステップ S 2 4、S 2 5、S 2 6 において、図 3 (A) のステップ S 1 2、S 1 3、S 1 4 における処理と同様の処理が行われる。すなわち、必要であれば T S 処理手段 3 0 0 によるトランスポートパケットに対する A T S 付加、暗号処理手段 1 5 0 における暗号化処理が実行され、その結果得られる暗号化コンテンツを、記録媒体 2 0 0 に記録して、記録処理を終了する。

【 0 0 6 5 】

次に、記録媒体 2 0 0 に記録されたコンテンツを再生して、デジタルコンテンツ、あるいはアナログコンテンツとして出力する処理について図 4 のフローに従って説明する。デジタルコンテンツとして外部に出力する処理は図 4 (A) のフローチャートにしたがった再生処理として実行される。即ち、まず最初に、ステップ S 3 1 において、記録媒体 I / F 1 9 0 によって、記録媒体 2 0 0 に記録さ

れた暗号化コンテンツが読み出され、バス 1 1 0 を介して、暗号処理手段 1 5 0 に出力される。

【 0 0 6 6 】

暗号処理手段 1 5 0 では、ステップ S 3 2 において、記録媒体 I / F 1 9 0 から供給される暗号化コンテンツが復号処理され、データがトランスポートストリームである場合は、復号データがバス 1 1 0 を介して、T S 処理手段 3 0 0 に出力され、T S 処理が不要の場合は入出力 I / F 1 2 0 に供給される。

【 0 0 6 7 】

T S 処理手段 3 0 0 は、ステップ S 4 3 において、トランスポートストリームを構成する各トランスポートパケットの A T S から出力タイミングを判定し、A T S に応じた制御を実行して、バス 1 1 0 を介して、入出力 I / F 1 2 0 に供給する。入出力 I / F 1 2 0 は、T S 処理手段 3 0 0 からのデジタルコンテンツを、外部に出力し、再生処理を終了する。なお、T S 処理手段 3 0 0 の処理、暗号処理手段 1 5 0 におけるデジタルコンテンツの復号処理については後述する。

【 0 0 6 8 】

さらに、データは入出力 I / F 1 2 0 に供給され、ステップ S 3 4 において、入出力 I / F 1 2 0 はデジタルコンテンツを、外部に出力し、再生処理を終了する。

【 0 0 6 9 】

なお、入出力 I / F 1 2 0 は、ステップ S 3 4 で、IEEE1394シリアルバスを介してデジタルコンテンツを出力する場合には、D T C P の規格に準拠して、上述したように、相手の装置との間で認証を相互に行い、その後、デジタルコンテンツを暗号化して伝送する。

【 0 0 7 0 】

記録媒体 2 0 0 に記録されたコンテンツを再生して、アナログコンテンツとして外部に出力する場合においては、図 4 (B) のフローチャートに従った再生処理が行われる。

【 0 0 7 1 】

即ち、ステップ S 4 1、S 4 2、S 4 3 において、図 4 (A) のステップ S 3

1、S32、S33における場合とそれぞれ同様の処理が行われ、これにより、暗号処理手段150において得られた復号されたデジタルコンテンツは、バス110を介して、MPEGコーデック130に供給される。

【0072】

MPEGコーデック130では、ステップS44において、デジタルコンテンツがMPEGデコード、すなわち伸長処理が実行され、入出力I/F140に供給される。入出力I/F140は、ステップS44において、MPEGコーデック130でMPEGデコードされたデジタルコンテンツを、内蔵するA/D、D/Aコンバータ141でD/A変換(S45)して、アナログコンテンツとする。そして、ステップS46に進み、入出力I/F140は、そのアナログコンテンツを、外部に出力し、再生処理を終了する。

【0073】

[トランスポートストリーム]

次に、図5を用いて、トランスポートストリームデータを処理する場合における記録媒体上のデータフォーマットを説明する。記録媒体上のデータの読み書きの最小単位をブロック(block)という名前と呼ぶ。1ブロックは、 $192 * X$ (エックス) バイト (例えば $X=32$) の大きさとなっている。

【0074】

例えばMPEG2のTS (トランスポート・ストリーム) パケット (188バイト) にATSを付加して192バイトとして、それをX個集めて1ブロックのデータとする。ATSは24乃至32ビットの着信時刻を示すデータであり、Arrival Time Stamp (着信時刻スタンプ) の略である。ATSは各パケットの着信時刻に応じたランダム性のあるデータとして構成される。記録媒体のひとつのブロック (セクタ) には、ATSを付加したTS (トランスポート・ストリーム) パケットをX個記録する。本発明の構成では、トランスポートストリームを構成する各ブロックの第1番目のTSパケットに付加されたATSを用いてそのブロック (セクタ) のデータを暗号化するブロックキーを生成する。

【0075】

ランダム性のあるATSを用いて暗号化用のブロックキーを生成することによ

り、ブロック毎に異なる固有キーが生成される。生成されたブロック固有キーを用いてブロック毎の暗号化処理を実行する。また、ATSを用いてブロックキーを生成する構成とすることにより、各ブロック毎の暗号化鍵を格納するための記録媒体上の領域が不要となり、メインデータ領域が有効に使用可能となる。さらに、データの記録、再生時にメインデータ部以外のデータをアクセスする必要もなくなり、処理が効率的になる。

【0076】

なお、図5に示すブロック・シード (Block Seed) は、ATSを含む付加情報である。ブロック・シードは、さらにATSだけでなく、図中段に示すようにコピー制限情報 (CCI : Copy Control Information) も付加する構成が可能である。この場合、ATSとCCIを用いてブロックキーを生成する構成とすることができる。

【0077】

なお、本発明の構成においては、DVD等の記録媒体上にデータを格納する場合、コンテンツの大部分のデータは暗号化されるが、図5の最下段に示すように、ブロックの先頭の m (たとえば、 $m=8$ または 16) バイトは暗号化されずに平文 (Unencrypted data) のまま記録され、残りのデータ ($m+1$ バイト以降) が暗号化される。これは暗号処理が8バイト単位としての処理であるために暗号処理データ長 (Encrypted data) に制約が発生するためである。なお、もし、暗号処理が8バイト単位でなく、たとえば1バイト単位で行なえるなら、 $m=4$ として、ブロックシード以外の部分をすべて暗号化してもよい。

【0078】

[TS処理手段における処理]

ここで、ATSの機能について詳細に説明する。ATSは、先にも説明したように入力トランスポートストリーム中の各トランスポートパケットの出現タイミングを保存するために付加する着信時刻スタンプである。

【0079】

すなわち、例えば複数のTVプログラム (コンテンツ) が多重化されたトランスポートストリームの中から1つまたは幾つかのTVプログラム (コンテンツ)

を取り出した時、その取り出したトランスポートストリームを構成するトランスポートパケットは、不規則な間隔で現れる（図 7（a）参照）。トランスポートストリームは、各トランスポートパケットの出現タイミングに重要な意味があり、このタイミングは M P E G 2 システムズ (ISO/IEC 13818-1) で規定されている仮想的なデコーダである T - S T D (Transport stream System Target Decoder) を破綻させないように符号化時に決定される。

【 0 0 8 0 】

トランスポートストリームの再生時には、各トランスポートパケットに付加された A T S によって出現タイミングが制御される。従って、記録媒体にトランスポートパケットを記録する場合には、トランスポートパケットの入力タイミングを保存する必要があり、トランスポートパケットを D V D 等の記録媒体に記録する時に、各トランスポートパケットの入力タイミングを表す A T S を付加して記録する。

【 0 0 8 1 】

図 6 に、デジタルインタフェース経由で入力されるトランスポートストリームを D V D 等の記録媒体であるストレージメディアに記録する時の T S 処理手段 3 0 0 において実行する処理を説明するブロック図を示す。端子 6 0 0 からは、デジタル放送等のデジタルデータとしてトランスポートストリームが入力される。図 1 においては、入出力 I / F 1 2 0 を介して、あるいは入出力 I / F 1 4 0、M P E G コーデック 1 3 0 を介して端子 6 0 0 からトランスポートストリームが入力される。

【 0 0 8 2 】

トランスポートストリームは、ビットストリームパーサー (parser) 6 0 2 に入力される。ビットストリームパーサー 6 0 2 は、入力トランスポートストリームの中から P C R (Program Clock Reference) パケットを検出する。ここで、P C R パケットとは、M P E G 2 システムズで規定されている P C R が符号化されているパケットである。P C R パケットは、1 0 0 m s e c 以内の時間間隔で符号化されている。P C R は、トランスポートパケットが受信側に到着する時刻を 2 7 M H z の精度で表す。

【 0 0 8 3 】

そして、27MHz PLL 603において、記録再生器が持つ27MHzクロックをトランスポートストリームのPCRにロック (Lock) させる。タイムスタンプ発生回路604は、27MHzクロックのクロックのカウント値に基づいたタイムスタンプを発生する。そして、ブロック・シード (Block seed) 付加回路605は、トランスポートパケットの第1バイト目がスミージングバッファ606へ入力される時のタイムスタンプをATSとして、そのトランスポートパケットに付加する。

【 0 0 8 4 】

ATSが付加されたトランスポートパケットは、スミージングバッファ606を通過して、端子607から、暗号処理手段150に出力され、後段で説明する暗号処理が実行された後、記録媒体I/F210 (図1) を介してストレージメディアである記録媒体200に記録される。

【 0 0 8 5 】

図7は、入力トランスポートストリームが記録媒体に記録される時の処理の例を示す。図7(a)は、ある特定プログラム (コンテンツ) を構成するトランスポートパケットの入力を示す。ここで横軸は、ストリーム上の時刻を示す時間軸である。この例ではトランスポートパケットの入力は、図7(a)に示すように不規則なタイミングで現れる。

【 0 0 8 6 】

図7(b)は、ブロック・シード (Block Seed) 付加回路605の出力を示す。ブロック・シード (Block Seed) 付加回路605は、トランスポートパケット毎に、そのパケットのストリーム上の時刻を示すATSを含むブロック・シード (Block Seed) を付加して、ソースパケットを出力する。図7(c)は記録媒体に記録されたソースパケットを示す。ソースパケットは、図7(c)に示すように間隔を詰めて記録媒体に記録される。このように間隔を詰めて記録することにより記録媒体の記録領域を有効に使用できる。

【 0 0 8 7 】

図8は、記録媒体200に記録されたトランスポートストリームを再生する場

合のTS処理手段300の処理構成ブロック図を示している。端子800からは、後段で説明する暗号処理手段において復号されたATS付きのトランスポートパケットが、ブロック・シード (Block seed) 分離回路801へ入力され、ATSとトランスポートパケットが分離される。タイミング発生回路804は、再生器が持つ27MHzクロック805のクロックカウンタ値に基づいた時間を計算する。

【0088】

なお、再生の開始時において、一番最初のATSが初期値として、タイミング発生回路804にセットされる。比較器803は、ATSとタイミング発生回路804から入力される現在の時刻を比較する。そして、タイミング発生回路804が発生する時間とATSが等しくなった時、出力制御回路802は、そのトランスポートパケットをMPEGコーデック130またはデジタル入出力I/F120へ出力する。

【0089】

図9は、入力AV信号を記録再生器100のMPEGコーデック130においてMPEGエンコードして、さらにTS処理手段300においてトランスポートストリームを符号化する構成を示す。従って図9は、図1におけるMPEGコーデック130とTS処理手段300の両処理構成を併せて示すブロック図である。端子901からは、ビデオ信号が入力されており、それはMPEGビデオエンコーダ902へ入力される。

【0090】

MPEGビデオエンコーダ902は、入力ビデオ信号をMPEGビデオストリームに符号化し、それをバッファビデオストリームバッファ903へ出力する。また、MPEGビデオエンコーダ902は、MPEGビデオストリームについてのアクセスユニット情報を多重化スケジューラ908へ出力する。ビデオストリームのアクセスユニットとは、ピクチャであり、アクセスユニット情報とは、各ピクチャのピクチャタイプ、符号化ビット量、デコードタイムスタンプである。ここで、ピクチャタイプは、I/P/Bピクチャ (picture) の情報である。また、デコードタイムスタンプは、MPEG2システムズで規定されている情報で

ある。

【 0 0 9 1 】

端子 9 0 4 からは、オーディオ信号が入力されており、それは M P E G オーディオエンコーダ 9 0 5 へ入力される。M P E G オーディオエンコーダ 9 0 5 は、入力オーディオ信号を M P E G オーディオストリームに符号化し、それをバッファ 9 0 6 へ出力する。また、M P E G オーディオエンコーダ 9 0 5 は、M P E G オーディオストリームについてのアクセスユニット情報を多重化スケジューラ 9 0 8 へ出力する。オーディオストリームのアクセスユニットとは、オーディオフレームであり、アクセスユニット情報とは、各オーディオフレームの符号化ビット量、デコードタイムスタンプである。

【 0 0 9 2 】

多重化スケジューラ 9 0 8 には、ビデオとオーディオのアクセスユニット情報が入力される。多重化スケジューラ 9 0 8 は、アクセスユニット情報に基づいて、ビデオストリームとオーディオストリームをトランスポートパケットに符号化する方法を制御する。多重化スケジューラ 9 0 8 は、内部に 2 7 M H z 精度の基準時刻を発生するクロックを持ち、そして、M P E G 2 で規定されている仮想的なデコーダモデルである T - S T D を満たすようにして、トランスポートパケットのパケット符号化制御情報を決定する。パケット符号化制御情報は、パケット化するストリームの種類とストリームの長さである。

【 0 0 9 3 】

パケット符号化制御情報がビデオパケットの場合、スイッチ 9 7 6 は a 側になり、ビデオストリームバッファ 9 0 3 からパケット符号化制御情報により指示されたペイロードデータ長のビデオデータが読み出され、トランスポートパケット符号化器 9 0 9 へ入力される。

【 0 0 9 4 】

パケット符号化制御情報がオーディオパケットの場合、スイッチ 9 7 6 は b 側になり、オーディオストリームバッファ 9 0 6 から指示されたペイロードデータ長のオーディオデータが読み出され、トランスポートパケット符号化器 9 0 9 へ入力される。

【0095】

パケット符号化制御情報がPCRパケットの場合、トランスポートパケット符号化器909は、多重化スケジューラ908から入力されるPCRを取り込み、PCRパケットを出力する。パケット符号化制御情報がパケットを符号化しないことを指示する場合、トランスポートパケット符号化器909へは何も入力されない。

【0096】

トランスポートパケット符号化器909は、パケット符号化制御情報がパケットを符号化しないことを指示する場合、トランスポートパケットを出力しない。それ以外の場合、パケット符号化制御情報に基づいてトランスポートパケットを生成し、出力する。したがって、トランスポートパケット符号化器909は、間欠的にトランスポートパケットを出力する。到着 (Arrival) タイムスタンプ (time stamp) 計算手段910は、多重化スケジューラ908から入力されるPCRに基づいて、トランスポートパケットの第1バイト目が受信側に到着する時刻を示すATSを計算する。

【0097】

多重化スケジューラ908から入力されるPCRは、MPEG2で規定されるトランスポートパケットの10バイト目の受信側への到着時刻を示すので、ATSの値は、PCRの時刻から10バイト前のバイトが到着する時刻となる。

【0098】

ブロック・シード (Block Seed) 付加回路911は、トランスポートパケット符号化器909から出力されるトランスポートパケットにATSを付加する。ブロック・シード (Block seed) 付加回路911から出力されるATS付きのトランスポートパケットは、スムージングバッファ912を通して、暗号処理手段150へ入力され、後段で説明する暗号処理が実行された後、ストレージメディアである記録媒体200へ格納される。

【0099】

記録媒体200へ格納されるATS付きのトランスポートパケットは、暗号処理手段150で暗号化される前に図7(c)に示すように間隔を詰めた状態で入

力され、その後、記録媒体200に格納される。トランスポートパッケージが間隔を詰めて記録されても、ATSを参照することによって、そのトランスポートパッケージの受信側への入力時刻を制御することができる。

【0100】

ところで、ATSの大きさは32ビットに決まっているわけではなく、24ビット乃至31ビットでも構わない。ATSのビット長が長いほど、ATSの時間カウンターが一周する周期が長くなる。例えば、ATSが27MHz精度のバイナリーカウンターである場合、24-bit長のATSが一周する時間は、約0.6秒である。この時間間隔は、一般のトランスポートストリームでは十分な大きさである。なぜなら、トランスポートストリームのパッケージ間隔は、MPEG2の規定により、最大0.1秒と決められているからである。しかしながら、十分な余裕を見て、ATSを24-bit以上にしても良い。

【0101】

このように、ATSのビット長を様々な長さとした場合、ブロックデータの付加データであるブロックシードの構成としていくつかの構成が可能となる。ブロック・シードの構成例を図10に示す。図10の例1は、ATSを32ビット分使用する例である。図10の例2は、ATSを30ビットとし、コピー制御情報(CCI)を2ビット分使用する例である。コピー制御情報は、それが付加されたデータのコピー制御の状態を表す情報であり、SCMS: Serial Copy Management SystemやCGMS: Copy Generation Management Systemが有名である。これらのコピー制御情報では、その情報が付加されたデータは制限なくコピーが許可されていることを示すコピーフリー(Copy Free)、1世代のみのコピーを許可する1世代コピー許可(One Generation Copy Allowed)、コピーを認めないコピー禁止(Copy Prohibited)などの情報が表せる。

【0102】

図10に示す例3は、ATSを24ビットとし、CCIを2ビット使用し、さらに他の情報を6ビット使用する例である。他の情報としては、たとえばこのデータがアナログ出力される際に、アナログ映像データのコピー制御機構であるマクロビジョン(Macrovision)のオン/オフ(On/Off)を示す情報など、様々な

情報を利用することが可能である。

【0103】

〔キー配信構成としてのツリー（木）構造について〕

次に、図1に示した記録再生装置が、データを記録媒体に記録、もしくは記録媒体から再生する際に必要なキー、例えばメディアキーを、各機器に配布する構成について説明する。図11は、本方式を用いた記録システムにおける記録再生装置の鍵の配布構成を示した図である。図11の最下段に示すナンバ0～15が個々の記録再生装置である。すなわち図11に示す木（ツリー）構造の各葉（リーフ：leaf）がそれぞれの記録再生装置に相当する。

【0104】

各デバイス0～15は、製造時（出荷時）に、あらかじめ定められている初期ツリーにおける、自分のリーフからルートに至るまでのノードに割り当てられた鍵（ノードキー）および各リーフのリーフキーを自身で格納する。図11の最下段に示すK0000～K1111が各デバイス0～15にそれぞれ割り当てられたリーフキーであり、最上段のKRから、最下段から2番目の節（ノード）に記載されたキー：KR～K111をノードキーとする。

【0105】

図11に示すツリー構成において、例えばデバイス0はリーフキーK0000と、ノードキー：K000、K00、K0、KRを所有する。デバイス5はK0101、K010、K01、K0、KRを所有する。デバイス15は、K1111、K111、K11、K1、KRを所有する。なお、図11のツリーにはデバイスが0～15の16個のみ記載され、ツリー構造も4段構成の均衡のとれた左右対称構成として示しているが、さらに多くのデバイスがツリー中に構成され、また、ツリーの各部において異なる段数構成を持つことが可能である。

【0106】

また、図11のツリー構造に含まれる各記録再生器には、様々な記録媒体、例えばDVD、CD、MD、メモリスティック（商標）等を使用する様々なタイプの記録再生器が含まれている。さらに、様々なアプリケーションサービスが共存することが想定される。このような異なるデバイス、異なるアプリケーションの

共存構成の上に図11に示すキー配布構成が適用されている。

【0107】

これらの様々なデバイス、アプリケーションが共存するシステムにおいて、例えば図11の点線で囲んだ部分、すなわちデバイス0, 1, 2, 3を同一の記録媒体を用いるひとつのグループとして設定する。例えば、この点線で囲んだグループ内に含まれるデバイスに対しては、まとめて、共通のコンテンツを暗号化してプロバイダから送付したり、共通に使用するマスターキーを送付したり、あるいは各デバイスからプロバイダあるいは決済機関等にコンテンツ料金の支払データをやはり暗号化して出力するといった処理が実行される。コンテンツプロバイダ、あるいは決済処理機関等、各デバイスとのデータ送受信を行なう機関は、図11の点線で囲んだ部分、すなわちデバイス0, 1, 2, 3を1つのグループとして一括してデータを送付する処理を実行する。このようなグループは、図11のツリー中に複数存在する。

【0108】

なお、ノードキー、リーフキーは、ある1つの鍵管理センタによって統括して管理してもよいし、各グループに対する様々なデータ送受信を行なうプロバイダ、決済機関等によってグループごとに管理する構成としてもよい。これらのノードキー、リーフキーは例えばキーの漏洩等の場合に更新処理が実行され、この更新処理は鍵管理センタ、プロバイダ、決済機関等が実行する。

【0109】

このツリー構造において、図11から明らかなように、1つのグループに含まれる3つのデバイス0, 1, 2, 3はノードキーとして共通のキーK00、K0、KRを保有する。このノードキー共有構成を利用することにより、例えば共通のマスターキーをデバイス0, 1, 2, 3のみに提供することが可能となる。たとえば、共通に保有するノードキーK00自体をマスターキーとして設定すれば、新たな鍵送付を実行することなくデバイス0, 1, 2, 3のみが共通のマスターキーの設定が可能である。また、新たなマスターキーKmasterをノードキーK00で暗号化した値Enc(K00, Kmaster)を、ネットワークを介してあるいは記録媒体に格納してデバイス0, 1, 2, 3に配布すれば、デバイス0, 1

、2、3のみが、それぞれのデバイスにおいて保有する共有ノードキーK00を用いて暗号Enc(K00, Kmaster)を解いてマスターキー: Kmasterを得ることが可能となる。なお、Enc(Ka, Kb)はKbをKaによって暗号化したデータであることを示す。

【0110】

また、ある時点tにおいて、デバイス3の所有する鍵: K0011, K001, K00, K0, KRが攻撃者(ハッカー)により解析されて露呈したことが発覚した場合、それ以降、システム(デバイス0, 1, 2, 3のグループ)で送受信されるデータを守るために、デバイス3をシステムから切り離す必要がある。そのためには、ノードキー: K001, K00, K0, KRをそれぞれ新たな鍵K(t)001, K(t)00, K(t)0, K(t)Rに更新し、デバイス0, 1, 2にその更新キーを伝える必要がある。ここで、K(t)aaaは、鍵Kaaaの世代(Generation): tの更新キーであることを示す。

【0111】

更新キーの配布処理について説明する。キーの更新は、例えば、図12(A)に示す有効化キーブロック(EKB: Enabling Key Block)と呼ばれるブロックデータによって構成されるテーブルをたとえばネットワーク、あるいは記録媒体に格納してデバイス0, 1, 2に供給することによって実行される。

【0112】

図12(A)に示す有効化キーブロック(EKB)には、ノードキーの更新に必要なデバイスのみが更新可能なデータ構成を持つブロックデータとして構成される。図12の例は、図11に示すツリー構造中のデバイス0, 1, 2において、世代tの更新ノードキーを配布することを目的として形成されたブロックデータである。図11から明らかなように、デバイス0、デバイス1は、更新ノードキーとしてK(t)00、K(t)0、K(t)Rが必要であり、デバイス2は、更新ノードキーとしてK(t)001、K(t)00、K(t)0、K(t)Rが必要である。

【0113】

図12(A)のEKBに示されるようにEKBには複数の暗号化キーが含まれ

る。最下段の暗号化キーは、 $Enc(K0010, K(t)001)$ である。これはデバイス2の持つリーフキー $K0010$ によって暗号化された更新ノードキー $K(t)001$ であり、デバイス2は、自身の持つリーフキーによってこの暗号化キーを復号し、 $K(t)001$ を得ることができる。また、復号により得た $K(t)001$ を用いて、図12(A)の下から2段目の暗号化キー $Enc(K(t)001, K(t)00)$ を復号可能となり、更新ノードキー $K(t)00$ を得ることができる。以下順次、図12(A)の上から2段目の暗号化キー $Enc(K(t)00, K(t)0)$ を復号し、更新ノードキー $K(t)0$ 、図12(A)の上から1段目の暗号化キー $Enc(K(t)0, K(t)R)$ を復号し $K(t)R$ を得る。一方、デバイス0, 1は、ノードキー $K000$ は更新する対象に含まれておらず、更新ノードキーとして必要なのは、 $K(t)00$ 、 $K(t)0$ 、 $K(t)R$ である。デバイス0, 1は、図12(A)の上から3段目の暗号化キー $Enc(K000, K(t)00)$ を復号し $K(t)00$ 、を取得し、以下、図12(A)の上から2段目の暗号化キー $Enc(K(t)00, K(t)0)$ を復号し、更新ノードキー $K(t)0$ 、図12(A)の上から1段目の暗号化キー $Enc(K(t)0, K(t)R)$ を復号し $K(t)R$ を得る。このようにして、デバイス0, 1, 2は更新した鍵 $K(t)R$ を得ることができる。なお、図12(A)のインデックスは、復号キーとして使用するノードキー、リーフキーの絶対番地を示す。

【0114】

図11に示すツリー構造の上位段のノードキー： $K(t)0, K(t)R$ の更新が不要であり、ノードキー $K00$ のみの更新処理が必要である場合には、図12(B)の有効化キーブロック(EKB: Enabling Key Block)を用いることで、更新ノードキー $K(t)00$ をデバイス0, 1, 2に配布することができる。

【0115】

図12(B)に示すEKBは、例えば特定のグループにおいて共有する新たなマスターキー、あるいは記録媒体に固有のメディアキーを配布する場合に利用可能である。具体例として、図11に点線で示すグループ内のデバイス0, 1, 2, 3がある記録媒体を用いており、新たな共通のマスターキー $K(t)master$ が

必要であるとする。このとき、デバイス 0, 1, 2, 3 の共通のノードキー K_{00} を更新した $K(t)_{00}$ を用いて新たな共通の更新マスターキー: $K(t)_{master}$ を暗号化したデータ $Enc(K(t), K(t)_{master})$ を図 12 (B) に示す EKB とともに配布する。この配布により、デバイス 4 など、その他のグループの機器においては復号されないデータとしての配布が可能となる。メディアキーについても同様である。

【0116】

すなわち、デバイス 0, 1, 2 は EKB を処理して得た $K(t)_{00}$ を用いて上記暗号文を復号すれば、 t 時点でのマスターキー: $K(t)_{master}$ やメディアキー: $K(t)_{media}$ を得ることが可能になる。

【0117】

[EKB を使用したメディアキーの取得]

図 13 に、本出願人の先の特許出願である特願平 2000-105328 で提案した t 時点でのメディアキー $K(t)_{media}$ を得る処理例として、 $K(t)_{00}$ を用いて新たな共通のメディアキー $K(t)_{media}$ を暗号化したデータ $Enc(K(t)_{00}, K(t)_{media})$ と図 12 (B) に示す EKB とを記録媒体を介して受領したデバイス 2 の処理を示す。

【0118】

図 11 に示すように、ある記録再生システムには、点線で囲まれた、デバイス 0, 1, 2, 3 の 4 つの装置が含まれるとする。図 13 は、デバイス 3 がリボークされたときに、記録媒体ごとに割り当てられるメディアキーを使用する場合に、記録再生装置 (デバイス 2) が記録媒体上のコンテンツを暗号化もしくは復号するために必要なメディアキーを、記録媒体に格納されている EKB (Enabling Key Block) と記録再生装置が記憶するデバイスキーを用いて求める際の処理を表している。

【0119】

デバイス 2 のメモリには、自分にのみ割り当てられたリーフキー K_{0010} と、それから木のルートまでの各ノード $001, 00, 0, R$ のノードキー (それぞれ、 $K_{001}, K_{00}, K_0, K_R$) が安全に格納されている。デバイス 2

は、図 1 3 の記録媒体に格納されている E K B のうち、インデックス (index) が 0 0 1 0 の暗号文を自分の持つリーフキー K_{0010} で復号してノード 0 0 1 のノードキー $K(t)_{001}$ を計算し、次にそれを用いてインデックス (index) が 0 0 1 の暗号文を復号してノード 0 0 のノードキー $K(t)_{00}$ を計算し、最後にそれを用いて暗号文を復号してメディアキー $K(t)_{media}$ を計算する必要がある。この計算回数は、リーフからメディアキーを暗号化するノードまでの深さが深くなるのに比例して増加する。すなわち、多くの記録再生装置が存在する大きなシステムにおいては多くの計算が必要となる。このようにして計算され、取得されたメディアキーを用いたデータの暗号化処理、復号処理態様について、以下、説明する。

【0 1 2 0】

〔メディアキーを用いたコンテンツ記録処理〕

図 1 4 の処理ブロック図に従って、暗号処理手段 1 5 0 が実行するデータの暗号化処理および記録媒体に対する記録処理の一例について説明する。

【0 1 2 1】

図 1 4 に示す記録再生装置 1 0 0 は自身の上述した E K B に基づく算出処理によってメディアキーを取得する。

【0 1 2 2】

次に、記録再生装置 1 0 0 は例えば光ディスクである記録媒体 2 0 0 に識別情報としてのディスク I D (Disc ID) が既に記録されているかどうかを検査する。記録されていれば、ディスク I D (Disc ID) を読出し、記録されていなければ、暗号処理手段 1 5 0 においてランダムに、もしくはあらかじめ定められた例えば乱数発生等の方法でディスク I D (Disc ID) を生成し、ディスクに記録する。ディスク I D (Disc ID) はそのディスクにひとつあればよいので、リードインエリアなどに格納することも可能である。

【0 1 2 3】

記録再生器 1 0 0 は、次にメディアキーとディスク I D を用いて、ディスク固有キー (Disc Unique Key) を生成する。ディスク固有キー (Disc Unique Key) の具体的な生成方法としては、図 1 5 に示すように、ブロック暗号関数を用いた

ハッシュ関数にメディアキーとディスクID (Disc ID) を入力して得られた結果を用いる例1の方法や、FIPS 180-1で定められているハッシュ関数SHA-1に、メディアキーとディスクID (Disc ID) とのビット連結により生成されるデータを入力し、その160ビットの出力から必要なデータ長のみをディスク固有キー (Disc Unique Key) として使用する例2の方法が適用できる。

【0124】

次に、記録ごとの固有鍵であるタイトルキー (Title Key) を暗号処理手段150 (図1参照) においてランダムに、もしくはあらかじめ定められた例えば乱数発生等の方法で生成し、ディスク200に記録する。

【0125】

次にディスク固有キー (Disc Unique Key) とタイトルキー (Title Key) の組合せから、タイトル固有キー (Title Unique Key) を生成する。

【0126】

このタイトル固有キー (Title Unique Key) 生成の具体的な方法は、図16に示すように、ブロック暗号関数を用いてディスク固有キーを鍵としてタイトルキーを暗号化して得られた結果を用いる例1の方法や、FIPS 180-1で定められているハッシュ関数SHA-1に、メディアキーとディスクID (Disc ID) とのビット連結により生成されるデータを入力し、その160ビットの出力から必要なデータ長のみをタイトル固有キー (Title Unique Key) として使用する例2の方法が適用できる。

【0127】

なお、上記の説明では、メディアキーとディスクID (Disc ID) からディスク固有キー (Disc Unique Key) を生成し、これとタイトルキー (Title Key) からタイトル固有キー (Title Unique Key) をそれぞれ生成するようにしているが、ディスク固有キー (Disc Unique Key) を不要としてメディアキーとディスクID (Disc ID) とタイトルキー (Title Key) から直接タイトル固有キー (Title Unique Key) を生成してもよく、また、タイトルキー (Title Key) を用いずに、メディアキー (Master Key) とディスクID (Disc ID) からタイトル固有キー (Title Unique Key) 相当の鍵を生成してもよい。

【 0 1 2 8 】

さらに、図 1 4 を用いて、その後の処理を説明する。被暗号化データとして入力されるブロックデータの先頭の第 1 ～ 4 バイトが分離されて出力されるブロックシード (Block Seed) と、先に生成したタイトル固有キー (Title Unique Key) とから、そのブロックのデータを暗号化する鍵であるブロック・キー (Block Key) が生成される。

【 0 1 2 9 】

ブロック・キー (Block Key) の生成方法の例を図 1 7 に示す。図 1 7 では、いずれも 3 2 ビットのブロック・シード (Block Seed) と、6 4 ビットのタイトル固有キー (Title Unique Key) とから、6 4 ビットのブロックキー (Block Key) を生成する例を 2 つ示している。

【 0 1 3 0 】

上段に示す例 1 は、鍵長 6 4 ビット、入出力がそれぞれ 6 4 ビットの暗号関数を使用している。タイトル固有キー (Title Unique Key) をこの暗号関数の鍵とし、ブロックシード (Block Seed) と 3 2 ビットの定数 (コンスタント) を連結した値を入力して暗号化した結果をブロックキー (Block Key) としている。

【 0 1 3 1 】

例 2 は、FIPS 180-1 のハッシュ関数 SHA-1 を用いた例である。タイトル固有キー (Title Unique Key) とブロックシード (Block Seed) を連結した値を SHA-1 に入力し、その 1 6 0 ビットの出力を、たとえば下位 6 4 ビットのみ使用するなど、6 4 ビットに縮約したものをブロックキー (Block Key) としている。

【 0 1 3 2 】

なお、上記ではディスク固有キー (Disc Unique key) 、タイトル固有キー (Title Unique Key) 、ブロックキー (Block Key) をそれぞれ生成する例を説明したが、たとえば、ディスク固有キー (Disc Unique Key) とタイトル固有キー (Title Unique Key) の生成を実行することなく、ブロックごとにメディアキーとディスク ID (Disc ID) とタイトルキー (Title Key) とブロックシード (Block Seed) を用いてブロックキー (Block Key) を生成してもよい。

【 0 1 3 3 】

ブロックキーが生成されると、生成されたブロックキー (Block Key) を用いてブロックデータを暗号化する。図 1 4 の下段に示すように、ブロックシード (Block Seed) を含むブロックデータの先頭の第 1 ~ m バイト (たとえば m = 8 バイト) は分離 (セクタ 1 6 0 8) されて暗号化対象とせず、m + 1 バイト目から最終データまでを暗号化する。なお、暗号化されない m バイト中にはブロック・シードとしての第 1 ~ 4 バイトも含まれる。セクタにより分離された第 m + 1 バイト以降のブロックデータは、暗号処理手段 1 5 0 に予め設定された暗号化アルゴリズムに従って暗号化される。暗号化アルゴリズムとしては、たとえば FI PS 46-2 で規定される D E S (Data Encryption Standard) を用いることができる。

【 0 1 3 4 】

以上の処理により、コンテンツはブロック単位で、世代管理されたメディアキー、ブロック・シード等に基づいて生成されるブロックキーで暗号化が施されて記録媒体に格納される。

【 0 1 3 5 】

次に、記録した暗号化コンテンツデータに対して、記録再生装置は自身に割り当てられた公開鍵暗号系の秘密鍵 (署名生成鍵) を用いてデジタル署名を計算し、これを自身の公開鍵証明書およびコンテンツデータと共に記録媒体に記録する。デジタル署名の生成方法としては、たとえば、IEEE P1363 で規格制定中の E C - D S A (Elliptic Curve Digital Signature Algorithm) を用いることができる。図 1 8 にコンテンツの記録処理の概要を説明するフローチャートを示す。

【 0 1 3 6 】

まず、記録再生装置はステップ S 1 0 1 において記録対象コンテンツの暗号化処理を実行する。コンテンツ暗号化は、図 1 4 を用いて説明したように、ブロックキーを用いたブロックデータの暗号化処理として実行される。

【 0 1 3 7 】

さらに、ステップ S 1 0 2 において、記録再生装置は自身に割り当てられた公開鍵暗号系の秘密鍵 (署名生成鍵) を用いて暗号化コンテンツに対するデジタル署名を計算する。デジタル署名の生成方法としては、たとえば、IEEE P1363 で

規格制定中の E C - D S A (Elliptic Curve Digital Signature Algorithm) が適用可能である。

【 0 1 3 8 】

次に、ステップ S 1 0 3 において、記録再生装置は生成したデジタル署名と公開鍵証明書を記録コンテンツに対応付けて記録媒体に記録し、ステップ S 1 0 4 において暗号化データの記録媒体に対する記録処理 (S 1 0 2) を実行する。

【 0 1 3 9 】

さらに、図 1 9 に暗号化コンテンツにデジタル署名を実行して記録を実行する場合の詳細処理フローを示す。

【 0 1 4 0 】

ステップ S 2 0 1 において、記録再生装置は前述の E K B 処理 (図 1 3 参照) によってメディアキーを取得する。

【 0 1 4 1 】

S 2 0 2 において、記録媒体に識別情報としてのディスク I D (Disc I D) が既に記録されているかどうかを検査する。記録されていれば S 2 0 3 でこのディスク I D を読出し、記録されていなければ S 2 0 4 で、ランダムに、もしくはあらかじめ定められた方法でディスク I D を生成し、ディスクに記録する。次に、S 2 0 5 では、メディアキーとディスク I D を用いて、ディスク固有キーを生成する。ディスク固有キーは先に説明したように、例えば、FIPS 180-1 で定められているハッシュ関数 S H A - 1 を用いる方法やブロック暗号に基づくハッシュ関数を使用する方法 (図 1 5 参照) などを適用することで求める。

【 0 1 4 2 】

次に S 2 0 6 に進み、その一回の記録ごとの固有の鍵としてのタイトルキー (Title Key) を生成し、生成したタイトルキーをディスク (記録媒体) に記録する。次に S 2 0 7 で、上記のディスク固有キーとタイトルキーとから、タイトル固有キーを生成 (図 1 6 参照) する。

【 0 1 4 3 】

S 2 0 8 では、記録再生装置は記録すべきコンテンツデータの被暗号化データを T S パケットの形で受信する。S 2 0 9 で、T S 処理手段 3 0 0 は、各 T S パ

ケットを受信した時刻情報であるATSを付加する。あるいはコピー制御情報CCIとATS、さらに他の情報を組み合わせた値を付加する。次に、S210で、ATSを付加したTS_PACKETを順次受信し、1ブロックを形成する例えばX=32に達したか、あるいはパケットの終了を示す識別データを受信したかを判定する。いずれかの条件が満足された場合はステップS211に進み、X個、あるいはパケット終了までのパケットを並べて、1ブロックのブロックデータを形成する。

【0144】

次に、暗号処理手段150は、S212で、ブロックデータの先頭の32ビット(ATSを含むブロック・シード)とS207で生成したタイトル固有キーとから、そのブロックのデータを暗号化する鍵であるブロックキーを生成(図17参照)する。

【0145】

S213では、ブロックキーを用いてS211で形成したブロックデータを暗号化する。なお、先にも説明したように、暗号化の対象となるのは、ブロックデータのm+1バイト目から最終データまでである。暗号化アルゴリズムは、たとえばFIPS 46-2で規定されるDES(Data Encryption Standard)が適用される。

【0146】

S214で、記録ブロックが第1ブロックであるか否かを判定し、第1ブロックである場合は、S215においてブロックデータをデジタル署名対象データとして、デジタル署名を生成し、公開鍵証明書とともに記録媒体に記録する。デジタル署名の生成処理は例えばIEEE P1363で規格制定中のECDSA(Elliptic Curve Digital Signature Algorithm)を適用する。

【0147】

S216で、暗号化したブロックデータを記録媒体に記録する。S217で、全データを記録したかを判断する。全データを記録していれば、記録処理を終了し、全データを記録していなければS208に戻って残りのデータの処理を実行する。

【 0 1 4 8 】

以上の処理により、コンテンツが暗号化されて記録媒体に記録され、さらに、暗号化コンテンツのブロックデータに対するデジタル署名、および公開鍵証明書が記録媒体に記録されることになる。

【 0 1 4 9 】

なお、記録媒体に格納されるコンテンツ、タイトルキー、デジタル署名、公開鍵証明書、その他コンテンツ関連データはそれぞれの対応が識別可能な構成をもって記録される。例えば管理データをテーブルとして記録媒体に記録することによって対応付けが可能である。図 2 0 に記録コンテンツに関する対応データのアドレスデータをテーブルとして記録する場合のテーブル構成例を示す。

【 0 1 5 0 】

図 2 0 に示すように、各コンテンツはコンテンツ関連データとともに、ファイルとして管理され、コンテンツデータのアドレス、タイトルキーのアドレス、デジタル署名のアドレス、公開鍵証明書のアドレス、その他ファイル情報について記録されたテーブルが生成され記録媒体に格納される。

【 0 1 5 1 】

次に、記録媒体に暗号化コンテンツを記録する際に、暗号化コンテンツに署名を実行するのではなく、コンテンツに対応して生成されるタイトルキーにデジタル署名を実行してコンテンツ記録を実行する処理について、図 2 1 のフローを用いて説明する。

【 0 1 5 2 】

ステップ S 3 0 1 において、記録再生装置は前述の E K B 処理（図 1 3 参照）によってメディアキーを取得する。

【 0 1 5 3 】

S 3 0 2 において、記録媒体に識別情報としてのディスク I D (Disc ID) が既に記録されているかどうかを検査する。記録されていれば S 3 0 3 でこのディスク I D を読出し、記録されていなければ S 3 0 4 で、ランダムに、もしくはあらかじめ定められた方法でディスク I D を生成し、ディスクに記録する。次に、S 3 0 5 では、メディアキーとディスク I D を用いて、ディスク固有キーを生成

する。ディスク固有キーは先に説明したように、例えば、FIPS 180-1で定められているハッシュ関数SHA-1を用いる方法やブロック暗号に基づくハッシュ関数を使用する方法（図15参照）などを適用することで求める。

【0154】

次にS306に進み、その一回の記録ごとの固有の鍵としてのタイトルキー（Title Key）を生成し、生成したタイトルキーに対するデジタル署名を実行する。デジタル署名の生成処理は例えばIEEE P1363で規格制定中のECDSA（Elliptic Curve Digital Signature Algorithm）を適用する。さらに、生成したタイトルキー、デジタル署名、および公開鍵証明書を記録媒体（ディスク）に格納する。

【0155】

次にS307で、上記のディスク固有キーとタイトルキーとから、タイトル固有キーを生成（図16参照）する。

【0156】

S308では、記録再生装置は記録すべきコンテンツデータの被暗号化データをTSパケットの形で受信する。S309で、TS処理手段300は、各TSパケットを受信した時刻情報であるATSを付加する。あるいはコピー制御情報CCIとATS、さらに他の情報を組み合わせた値を付加する。次に、S310で、ATSを付加したTSパケットを順次受信し、1ブロックを形成する例えばX=32に達したか、あるいはパケットの終了を示す識別データを受信したかを判定する。いずれかの条件が満足された場合はステップS311に進み、X個、あるいはパケット終了までのパケットを並べて、1ブロックのブロックデータを形成する。

【0157】

次に、暗号処理手段150は、S312で、ブロックデータの先頭の32ビット（ATSを含むブロック・シード）とS307で生成したタイトル固有キーとから、そのブロックのデータを暗号化する鍵であるブロックキーを生成（図17参照）する。

【0158】

S 3 1 3 では、ブロックキーを用いて S 3 1 1 で形成したブロックデータを暗号化する。なお、先にも説明したように、暗号化の対象となるのは、ブロックデータの $m + 1$ バイト目から最終データまでである。暗号化アルゴリズムは、たとえば FIPS 46-2 で規定される DES (Data Encryption Standard) が適用される。

【 0 1 5 9 】

S 3 1 4 で、暗号化したブロックデータを記録媒体に記録する。S 3 1 5 で、全データを記録したかを判断する。全データを記録していれば、記録処理を終了し、全データを記録していなければ S 3 0 8 に戻って残りのデータの処理を実行する。

【 0 1 6 0 】

以上の処理により、コンテンツが暗号化されて記録媒体に記録され、さらに、暗号化コンテンツに対応するタイトルキーに対するデジタル署名、および公開鍵証明書が記録媒体に記録されることになる。

【 0 1 6 1 】

上記の例ではタイトルキーにデジタル署名を施したが、タイトルキーとディスク ID に対してデジタル署名を施してもよい。このようにすることにより、そのデータがそのディスクに記録されたということを明確にでき、そのデータが他のディスクにコピーされたものは不正なコピーであるという判断が容易に行える。

【 0 1 6 2 】

【メディアキーを用いたコンテンツ再生処理】

次に、記録媒体に格納された暗号化コンテンツデータの復号および再生処理を図 2 2 以下を用いて説明する。

【 0 1 6 3 】

再生処理においては、再生装置はまず、再生するコンテンツデータと共に記録されている記録装置の公開鍵証明書とデジタル署名を讀出し、これらの正当性を確認する。

【 0 1 6 4 】

すなわち、再生装置が保持している、信頼できるセンタの公開鍵（署名検証鍵

）を用いて公開鍵証明書の正当性を検査し、これに成功すれば、公開鍵証明書に含まれている、記録装置の公開鍵（署名検証鍵）を用いて記録装置が作成して記録したデジタル署名を検査する。デジタル署名の検査方法としては、たとえば、前述のE C - D S Aを用いることができる。

【0165】

次に、再生装置は、記録されている公開鍵証明書から記録装置の識別情報（ID）を読み出し、これとリボケーション情報からこの記録装置がシステムからリボーク（排除）されていないことを確認する。

【0166】

（リボケーションリストを用いたリボーク検査）

リボケーション情報としては、たとえば図23に示すリボケーションリストを用いることができる。リボケーションリストは図に示すようにリボーク（排除）する機器のIDを併記したデータと、リストのバージョンナンバーに対してセンタがデジタル署名を施したものである。このリボケーションリストは、たとえば、1）製造される機器（記録再生装置）のメモリに記憶させる。さらに、2）コンテンツデータと一緒にネットワークや記録媒体を介して流通させる。などの方法で、システム内を流通させることにより、再生処理時に再生装置がより新しいリボケーション情報を得られるようにしておく。

【0167】

また、リボケーションリストを使用する際には、リストが偽造、改ざんされたものでないことを検査するために、リボケーションリスト内に格納されたセンタの署名の検証処理を実行する。署名の検証処理は、公開鍵証明書の署名検証と同様、予め機器（記録再生装置）が持っているセンタの公開鍵（署名検証鍵）を用いて検査することが可能である。

【0168】

（E K B を利用したリボーク検査）

また、リボケーション情報を図23に示すようなリストとして各機器に配布する構成をとらず、リボークされているか否かをE K B を使用して判別する構成としてもよい。たとえば図11に示したツリー状に機器が配置されたシステムにお

いて、図 1 2 の (A) 例 1 に示す E K B が記録媒体に格納されていたとする。このとき、各機器は、E K B のインデックスを逐次みていくと、E K B で更新されるノードキーをツリー状に表したものが図 2 4 の太線のようになることが理解できる。

【 0 1 6 9 】

そして、更新されたノードキーを得られるのは、太線で示したツリーのリーフ（葉）の下に位置する機器だけ、つまり、デバイス 0, 1, 2 だけであることが理解できる。そして、それ以外の機器はシステムからリボークされていると判断することができ、これらの I D を持った機器が記録したコンテンツデータの再生を禁止する処理を、再生処理の実行時に実行することによりリボーク機器による記録コンテンツの再配布を停止することが可能となる。なお、この例では、図 1 1 におけるリーフの位置と、デバイスの I D が対応していることを前提としている。すなわち、有効化キープロック（E K B）のインデックスのトレース処理を前記 I D に基づいて実行することでリボークの有無を判別する。

【 0 1 7 0 】

トレース処理によるリボーク検査について詳細に説明する。まず、図 2 5 に有効化キープロック（E K B）のフォーマット例を示す。バージョン 1 0 0 1 は、有効化キープロック（E K B）のバージョンを示す識別子である。なお、バージョンは最新の E K B を識別する機能とコンテンツとの対応関係を示す機能を持つ。デプス 1 0 0 2 は、有効化キープロック（E K B）の配布先のデバイスに対する階層ツリーの階層数を示す。データポインタ 1 0 0 3 は、有効化キープロック（E K B）中のデータ部の位置を示すポインタであり、タグポインタ 1 0 0 4 はタグ部の位置、署名ポインタ 1 0 0 5 は署名の位置を示すポインタである。

【 0 1 7 1 】

データ部 1 0 0 6 は、例えば更新するノードキーを暗号化したデータを格納する。例えば図 1 3 に示すような更新されたノードキーに関する各暗号化キー等を格納する。

【 0 1 7 2 】

タグ部 1 0 0 7 は、データ部に格納された暗号化されたノードキー、リーフキ

一の位置関係を示すタグである。このタグの付与ルールを図26を用いて説明する。図26では、データとして先に図12(A)で説明した有効化キーブロック(ENB)を送付する例を示している。この時のデータは、図26の表(b)に示すようになる。このときの暗号化キーに含まれるトップノードのアドレスをトップノードアドレスとする。この場合は、ルートキーの更新キー $K(t)R$ が含まれているので、トップノードアドレスは KR となる。このとき、例えば最上段のデータ $Enc(K(t)0, K(t)R)$ は、図26の(a)に示す階層ツリーに示す位置にある。ここで、次のデータは、 $Enc(K(t)00, K(t)0)$ であり、ツリー上では前のデータの左下の位置にある。データがある場合は、タグが0、ない場合は1が設定される。タグは{左(L)タグ, 右(R)タグ}として設定される。最上段のデータ $Enc(K(t)0, K(t)R)$ の左にはデータがあるので、Lタグ=0、右にはデータがないので、Rタグ=1となる。以下、すべてのデータにタグが設定され、図26(c)に示すデータ列、およびタグ列が構成される。

【0173】

タグは、データ $Enc(Kxxx, Kyyy)$ がツリー構造のどこに位置しているのかを示すために設定されるキー配置識別タグである。データ部に格納されるキーデータ $Enc(Kxxx, Kyyy)...$ は、単純に暗号化されたキーの羅列データに過ぎないので、上述したタグによってデータとして格納された暗号化キーのツリー上の位置を判別可能としたものである。上述したタグを用いずに、先の図12で説明した構成のように暗号化データに対応させたノード・インデックスを用いて、例えば、

0: $Enc(K(t)0, K(t)root)$

00: $Enc(K(t)00, K(t)0)$

000: $Enc(K((t)000, K(T)00)$

...のようなデータ構成とすることも可能であるが、このようなインデックスを用いた構成とすると冗長なデータとなりデータ量が増大し、ネットワークを介する配信等においては好ましくない。これに対し、上述したタグをキー位置を示す索引データとして用いることにより、少ないデータ量でキー位置の判別が可

能となる。

【0174】

図25に戻って、EKBフォーマットについてさらに説明する。署名 (Signature) は、有効化キープロック (EKB) を発行したEKB発行局、例えば認証局、鍵管理センタ、コンテンツロバイダ、決済機関等が実行する電子署名である。EKBを受領したデバイスは署名検証によって正当な有効化キープロック (EKB) 発行者が発行した有効化キープロック (EKB) であることを確認する。

【0175】

図26に関する説明から理解されるようにEKB内に格納されたタグは自ノードの左及び右のノードの鍵データの有無を0, 1で示している。すなわちデータがある場合は0、データがない場合を1として設定される。リーフIDに基づくEKBの追跡処理、すなわち辿り方は、このような条件設定に基づくタグを用いて行われる。

【0176】

リーフIDに基づくEKBの追跡 (辿り方) について、図27を用いて説明する。図27(a)に示すようにリーフキーK1001を持つデバイスをリボークデバイス [1001] とする。このとき、EKBは、図27(b)のような暗号化キーとタグの構成を持つ。図27(b)のEKBは、図27(a)の1つのデバイス [1001] をリボークするために、KR, K1, K10, K100を更新したEKBとなる。

【0177】

このEKBを処理することにより、リボークデバイス [1001] 以外のリーフはすべて更新されたルートキーK(t)Rを取得できる。すなわち、ノードキーK0の下位につらなるリーフは、更新されていないノードキーK0をデバイス内に保持しているので、Enc(K0, K(t)R)をK0によって復号することで更新ルートキーK(t)Rを取得可能となる。また、K11以下のリーフは更新されていないK11を用いて、Enc(K11, K(t)1)をK11によって復号することで更新ノードキーK(t)1を取得して、さらに、Enc(K(t)1, K(t)R)をK(t)1によって復号することで更新ルートキーを

取得できる。K 1 0 1 の下位リーフについても復号ステップが 1 つ増加するのみで、同様に更新ルートキーを取得できる。

【 0 1 7 8 】

また、リボークされていないリーフキー K 1 0 0 0 を持つデバイス [1 0 0 0] は、自己のリーフキーで、 $Enc(K 1 0 0 0, K(t) 1 0 0)$ を復号して、 $K(t) 1 0 0$ を取得後、上位のノードキーを順次復号して更新ルートキーを取得できる。

【 0 1 7 9 】

リボークされたデバイス [1 0 0 1] のみが、自己のリーフの一段上の更新ノードキー $K(t) 1 0 0$ を EKB 処理により取得できないので、結局、更新ルートキー $K(t) R$ を取得することができない。

【 0 1 8 0 】

リボークされていない正当なデバイスには、図 2 7 (b) に示すデータ部と、タグを有する EKB が EKB 発行局から配信され、デバイス内に格納されている。

【 0 1 8 1 】

リボーク検証を行なおうとするデバイスは、図 2 7 (a) のリボークデバイス [ID = 1 0 0 1] の公開鍵証明書の検証の後、公開鍵証明書から ID を取得する。この ID は [1 0 0 1] であり、EKB 配信ツリー構成のリーフ位置を示している。

【 0 1 8 2 】

ID [1 0 0 1] を取り出したデバイスは、ID = 1 0 0 1 のリーフに対応するデバイスが、EKB において有効なリーフデバイスとして設定されているかを検証する。この検証は、すなわち、リーフ [1 0 0 1] が更新されたルートキー $K(t) R$ を取得できるか否かを判定する処理として実行される。

【 0 1 8 3 】

例えば、非更新ノードキー (ex. 図 2 7 (a) の K 0, K 1 1 など) の下位に属するリーフであれば、リボークされていないことが明らかであり、正当デバイスであると判定可能であり、更新ノードキーの下位に属するリーフである場合

は、その更新ノードキーを取得可能な暗号化データがEKBに格納されているか否かによって、そのエンティティがリボークされているか否かを判定可能となる。

【0184】

判定処理の一例として、EKBに格納されたタグに基づいてEKB追跡処理を行なう例を説明する。EKB追跡処理は、上位のルートキーからキー配信ツリーを辿れるか否かを判定する処理である。例えば図27のリーフ[1001]のIDである[1001]を[1]、[0]、[0]、[1]の4ビットとして、最上位ビットから順次下位ビットに従ってツリーを辿る。ビットが1であれば右側、0であれば左に進む。

【0185】

図27(a)のルートから、ID[1001]の最上位ビットは1であり、右側に進む。EKB内の最初のタグは、0:{0,0}であり、両枝にデータを有することが判定され、右側に進みK1に辿り着ける。次にK1の下位のノードに進む。ID[1001]の2番目のビットは0であり、左側に進む。K1の下位のデータ有無を示すタグは、図27(a),(b)の2:{0,0}であり、両枝にデータを有すると判定され、左側に進みK10に辿り着ける。さらに、ID[1001]の3番目のビットは0であり、左側に進む。K10の下位のデータ有無を示すタグは、図27(a),(b)の3:{0,0}であり、両枝にデータを有すると判定され、左側に進みK100に辿り着ける。さらに、ID[1001]の最下位ビットは1であり、右側に進む。K100の下位のデータ有無を示すタグは、図27(a),(b)の5:{0,1}であり、右側にはデータを持たない。従ってノード[1001]には辿りつけないことが判定され、ID[1001]のデバイスはEKBによる更新ルートキーを取得できないデバイス、すなわちリボークデバイスであると判定される。

【0186】

例えば図27(a)のリーフキーK1000を有するデバイスIDは[1000]であり、上述と同様のEKB内のタグに基づくEKB追跡処理、すなわちツリーを辿る処理を実行すると、ノード[1000]に辿りつくことができるので

、EKBによる更新ルートキーを取得可能なりボークされていない正当なデバイスであると判定される。

【0187】

また、例えば更新されていないノードキー、例えばK0、K11などの下位のリーフにも、リーフ自体には、辿り着けないが、この場合は、更新されていない末端ノードに辿りつくことが可能である。更新されていないノードの下位のリーフは、更新されていないノードキーを用いてEKBの処理が可能であり、更新ルートキーを取得できるので正当なデバイスである。更新されていないノードキーであるか否かは、そのノードに対応するタグにより判定することが可能となる。更新されていないノードキーK0、K11、K101に対応するタグは1：{1，1}、4：{1，1}、6 {1，1} となり、これらはさらに下位ノードまたはリーフが存在するが、EKB内には暗号化鍵データを持たないことを示しており、これらの下位のリーフのデバイスはリボークされていない有効な正当デバイスであると判定される。

【0188】

図27に示す例は、1つのデバイスについてのみのリボーク態様であるが、図28に示すようにあるノードの下にあるすべてのリーフデバイスを一括してリボークすることも可能である。この場合のEKBのデータ（暗号化キー）、タグは図28（b）のようになる。

【0189】

例えば、デバイスがリボークされたK1000に対応するリーフデバイスの公開鍵証明書からID [1000] を取得したとすると、このID [1000] に基づいてEKBのタグに基づいてツリーを辿る処理を実行する。

【0190】

図28（a）のルートから、ID [1000] の最上位ビットは1であり、右側に進む。EKB内の最初のタグ0：{0，0} であり、両枝にデータを有することが判定され、右側に進みK1に辿り着ける。次にK1の下位のノードに進む。ID [1000] の2番目のビットは0であり、左側に進む。K1の下位のデータ有無を示すタグは、図13（a），（b）の2：{1，0} であり、左側に

はデータを持たない。従ってノード [1 0 0 0] には辿りつけない。このときの末端ノード K 1 に対応するタグは {1, 0} であり、下位のデータを持たない {1, 1} ではない。

【0 1 9 1】

タグ {1, 0} は、K 1 の右側の下位のノードまたはリーフにおいてのみ復号可能な更新された K 1 (t) を取得するための暗号化鍵データが E K B に格納されていることを示している。

【0 1 9 2】

このように、リーフ I D に基づいて辿り着く最終地点がノードであり、その最終ノードの対応タグが {1, 1} 以外の値を持っている場合は、さらに下位の暗号化鍵データを E K B 内に有することを示している。この場合は、その I D を持つリーフデバイスは E K B の処理によって更新されたルートキーを取得することができないので、リボークされたデバイスであると判定される。

【0 1 9 3】

このようにして、認証処理において通信相手から取得した公開鍵証明書に格納されたリーフ I D に基づいて通信相手がリボークされているか否かを判定することが可能となる。

【0 1 9 4】

図 2 9 に E K B を利用したリボークデバイス判定処理についての処理フローを示す。フローの各ステップについて説明する。ステップ S 3 5 1 において、検査対象の公開鍵証明書から I D を取得する。ステップ S 3 5 2 において、取得した I D を用い E K B のタグに基づいて、I D の示すリーフまたはリードを目標とする追跡処理を実行する。

【0 1 9 5】

追跡処理は、前述の図 2 7, 図 2 8 を用いて説明した手順で実行する。追跡処理の結果、I D の示すリーフまたはノードに辿り着くことができたか、辿りつけない場合であっても I D の示すリーフまたはノードにおいて E K B 処理が可能であるか否か、すなわち更新ルートキーの取得が可能か否かを判定する (S 3 5 3)。

【0196】

E K B 処理が可能である位置にある I D であると判定されれば、ステップ S 3 5 4 に進み、I D に対応するデバイスはリボークされていない正当なデバイスであると判定する。一方、E K B 処理が不可能な位置にある I D であると判定されれば、ステップ S 3 5 5 に進み、I D に対応するデバイスはリボークされている不正なデバイスであると判定する。

【0197】

なお、上述の追跡処理では、E K B のタグ部は利用しているがデータ部は利用していない。これを用いて、リボケーション情報を表す目的では、図 2 5 に示す通常の E K B ではなく、データ部のない E K B を用いることにより、それ用の E K B のサイズを小さくできる。もちろん、図 2 5 に示す、通常の、コンテンツを保護するための E K B をリボケーション情報を表すために用いることも可能である。

【0198】

上述したように、リボケーションリスト、あるいは E K B ツリーのトレース処理に従ったリボーク検査により記録媒体に対してコンテンツの記録を行なった機器がリボークされているかいないかの検証を行なう。コンテンツの記録を行なった機器がリボークされてないことが検証されたことを条件として再生装置はコンテンツデータの再生処理を継続する。再生処理においては、図 1 4 を用いて説明した暗号化および記録処理と同様、メディアキーとディスク I D からディスク固有キーを生成し、ディスク固有キーと、タイトルキーからタイトル固有キーを生成し、さらにタイトルキーと記録媒体から読み取られるブロックシードとから、ブロックキーを生成して、ブロックキーを復号キーとして用い、記録媒体 2 0 0 から読み取られるブロック単位の暗号化データの復号処理を実行する。

【0199】

再生処理の概要について図 3 0 のフローチャートを用いて説明する。まず、ステップ S 4 0 1 において再生装置は、再生対象コンテンツを記録した記録媒体に格納されたコンテンツ記録装置の公開鍵証明書およびデジタル署名の検証を実行する。検証は、まず、公開鍵証明書のセンタ署名をセンタの公開鍵を用いて実

行し、公開鍵証明書 の 正当性が確認された後、公開鍵証明書中に格納されたコンテンツ記録装置の公開鍵を取り出して、コンテンツ記録者のデジタル署名の検証を実行する。いずれの検証も OK であれば次ステップに進み、いずれかの検証が NG であれば、以降のステップ実行が禁止され再生処理はストップする。

【 0 2 0 0 】

次に、ステップ S 4 0 2 においてコンテンツ記録装置のリボケーション検査を実行する。このリボケーション検査は、例えば予め再生装置に格納された図 2 3 に示したリボケーションリストに格納された機器 ID と、公開鍵証明書内の機器 ID に一致するものがあるか否かを検査することによって行われる。あるいは、前述の E K B ツリー構成によるツリー探索処理を実行してもよい。ステップ S 4 0 2 のリボケーション検査においてコンテンツ記録装置がリボークされていないと判定されると次ステップに進み、リボークされている場合は、以降のステップ実行が禁止され再生処理はストップする。

【 0 2 0 1 】

ステップ S 4 0 2 のリボケーション検査においてコンテンツ記録装置がリボークされていないと判定された場合、ステップ S 4 0 3 において暗号化コンテンツの記録媒体からの読み出しが実行され、ステップ S 4 0 4 において暗号化コンテンツの復号処理が実行されてコンテンツの再生が行われる。

【 0 2 0 2 】

このように、記録媒体に格納されたコンテンツ再生処理に際し、コンテンツ記録装置のリボーク状況を判定してリボークされていない機器によって記録されたコンテンツの再生のみを実行する構成としたので、不正に記録されたコンテンツが無秩序に流通利用されることが防止される。また、リボーク判定は、公開鍵証明書に格納された ID によって判定され、その信頼性は維持される。

【 0 2 0 3 】

次に、図 3 1 を用いて暗号化コンテンツに対してデジタル署名が実行された記録コンテンツの再生を実行する場合の詳細処理について説明する。

【 0 2 0 4 】

ステップ S 5 0 1 において、再生装置は記録媒体からメディアキー、ディスク

IDを読み出し、ステップS502において、タイトルキー、デジタル署名、公開鍵証明書の読み出しを実行する。署名、公開鍵証明書が存在しない場合（S503：No）は、正当な記録処理によるコンテンツではないと判定され、以降の処理の実行が停止され再生処理は終了する。

【0205】

署名、公開鍵証明書が存在した場合（S503：Yes）は、ステップS504において公開鍵証明書の検証が実行される。公開鍵証明書の検証は、再生装置が保有する公開鍵証明書の発行管理を行なうセンタ（認証局）の公開鍵を用いて実行される。公開鍵証明書の検証がOKであり正当性が確認されると次ステップに進む。正当性検証がNGの場合は、以降の処理の実行が停止され再生処理は終了する。

【0206】

次に、ステップS505では、公開鍵証明書からコンテンツ記録を実行した記録装置の識別子（ID）が取り出され、リボーク検査を行なう。リボーク検査は前述の図23のリボークリストあるいはツリー探索処理のいずれかによって実行される。コンテンツの記録装置のリボークがないと判定されると次ステップに進み、リボークありと判定されると、以降の処理の実行が停止され再生処理は終了する。

【0207】

次に、S506では、メディアキーとディスクIDを用いて、ディスク固有キーを生成する。ディスク固有キーは先に説明したように、例えば、FIPS 180-1で定められているハッシュ関数SHA-1を用いる方法やブロック暗号に基づくハッシュ関数を使用する方法（図15参照）などを適用することで求める。

【0208】

次にS507に進みタイトルキー（Title Key）を読み出し、読み出したタイトルキーとディスク固有キーから、タイトル固有キーを生成（図16参照）する。

【0209】

S508では、再生装置は再生すべきコンテンツデータのブロックデータを読

み出す。S 5 0 9 で読み出しブロックが第1ブロックであるか否かを判定し、第1ブロックである場合には、ステップS 5 1 0 において第1ブロックに対して生成されたコンテンツ記録者（記録装置）のデジタル署名の検証を実行する。デジタル署名の検証は、正当性の検証された公開鍵証明書から取り出したコンテンツ記録装置の公開鍵を用いて実行される。デジタル署名の検証がOKであり正当性が確認されると次ステップに進む。正当性検証がNGの場合は、以降の処理の実行が停止され再生処理は終了する。

【 0 2 1 0 】

ステップS 5 1 1 では、ブロックデータの先頭の32ビット（ATSを含むブロック・シード）とS 5 0 7 で生成したタイトル固有キーとから、そのブロックのデータを復号する鍵であるブロックキーを生成（図17参照）する。

【 0 2 1 1 】

S 5 1 2 では、ブロックキーを用いてブロックデータを復号する。復号アルゴリズムは、たとえばFIPS 46-2で規定されるDES（Data Encryption Standard）が適用される。

【 0 2 1 2 】

S 5 1 3 で、全データを読み出したかを判断する。全データを読み出していれば、再生処理を終了し、全データを読み出していなければS 5 0 8 に戻って残りのデータの処理を実行する。

【 0 2 1 3 】

このように、公開鍵証明書の検証、コンテンツ記録装置のリボークの判定、暗号化コンテンツのブロックデータに対するデジタル署名の検証が順次実行され、すべての条件が満足したことに基づいてコンテンツの正当性が判定され、暗号化コンテンツの記録媒体からの復号、再生処理が実行されることになる。

【 0 2 1 4 】

次に、図32を用いてタイトルキーに対してデジタル署名が実行された記録コンテンツの再生を実行する場合の詳細処理について説明する。

【 0 2 1 5 】

ステップS 6 0 1 において、再生装置は記録媒体からメディアキー、ディスク

IDを読み出し、ステップS602において、タイトルキー、デジタル署名、公開鍵証明書の読み出しを実行する。署名、公開鍵証明書が存在しない場合（S603：No）は、正当な記録処理によるコンテンツではないと判定され、以降の処理の実行が停止され再生処理は終了する。

【0216】

署名、公開鍵証明書が存在した場合（S603：Yes）は、ステップS604において公開鍵証明書の検証が実行される。公開鍵証明書の検証は、再生装置が保有する公開鍵証明書の発行管理を行なうセンタ（認証局）の公開鍵を用いて実行される。公開鍵証明書の検証がOKであり正当性が確認されると次ステップに進む。正当性検証がNGの場合は、以降の処理の実行が停止され再生処理は終了する。

【0217】

次に、ステップS605では、公開鍵証明書からコンテンツ記録を実行した記録装置の識別子（ID）が取り出され、リボーク検査を行なう。リボーク検査は前述の図23のリボークリストあるいはツリー探索処理のいずれかによって実行される。コンテンツの記録装置のリボークがないと判定されると次ステップに進み、リボークありと判定されると、以降の処理の実行が停止され再生処理は終了する。

【0218】

次に、ステップS606においてタイトルキーに対して実行されたコンテンツ記録者（記録装置）のデジタル署名の検証を実行する。デジタル署名の検証は、正当性の検証された公開鍵証明書から取り出したコンテンツ記録装置の公開鍵を用いて実行される。デジタル署名の検証がOKであり正当性が確認されると次ステップに進む。正当性検証がNGの場合は、以降の処理の実行が停止され再生処理は終了する。

【0219】

次に、S607では、メディアキーとディスクIDを用いて、ディスク固有キーを生成する。ディスク固有キーは先に説明したように、例えば、FIPS 180-1で定められているハッシュ関数SHA-1を用いる方法やブロック暗号に基づくハ

ッシュ関数を使用する方法（図15参照）などを適用することで求める。

【0220】

次にS608に進みタイトルキー（Title Key）を読み出し、読み出したタイトルキーとディスク固有キーから、タイトル固有キーを生成（図16参照）する。

【0221】

S609では、再生装置は再生すべきコンテンツデータのブロックデータを読み出す。ステップS610では、ブロックデータの先頭の32ビット（ATSを含むブロック・シード）とS608で生成したタイトル固有キーとから、そのブロックのデータを復号する鍵であるブロックキーを生成（図17参照）する。

【0222】

S611では、ブロックキーを用いてブロックデータを復号する。復号アルゴリズムは、たとえばFIPS 46-2で規定されるDES（Data Encryption Standard）が適用される。

【0223】

S612で、全データを読み出したかを判断する。全データを読み出していれば、再生処理を終了し、全データを読み出していなければS609に戻って残りのデータの処理を実行する。

【0224】

このように、公開鍵証明書の検証、コンテンツ記録装置のリボークの判定、暗号化コンテンツのタイトルキーに対するデジタル署名の検証が順次実行され、すべての条件が満足したことに基づいてコンテンツの正当性が判定され、暗号化コンテンツの記録媒体からの復号、再生処理が実行されることになる。

【0225】

上述のように、コンテンツデータの記録媒体に対する記録時の暗号化処理、および記録媒体からの再生時の復号処理においては、EKBに基づいてメディアキーを算出し、その後算出したメディアキーと他の識別子等に基づいて、コンテンツの暗号化処理用の鍵、または復号処理用の鍵を生成する。

【0226】

なお、上述した例では、メディアキーを用いてコンテンツデータの暗号化処理、および復号処理に用いるキーを生成する構成を説明したが、メディアキーではなく、複数の記録再生装置に共通のマスターキー、あるいは記録再生器固有のデバイスキーをEKBから取得して、これらに基づいてコンテンツデータの暗号化処理、および復号処理に用いるキーを生成する構成としてもよい。さらに、EKBから取得されるメディアキー、マスターキー、あるいはデバイスキー自体をコンテンツデータの暗号化処理、および復号処理に用いるキーとして適用することも可能である。

【0227】

上述のように、本発明においては、記録再生装置がデータを情報記録媒体に記録する際に自身のデジタル署名および公開鍵証明書をデータと共に記録するようにした。このことにより、情報を記録する際には、必ず、どの記録装置が記録したかという証拠もデータと共に記録するようにしているので、もし不正に記録されたデータを含む記録媒体が流通したとしても、それをどの記録装置が記録したか特定できるので、システムからの排除が行える。

【0228】

さらに、記録再生装置がデータを読み出す際に上記デジタル署名および公開鍵証明書の正当性を確認し、さらに記録装置がシステムからリボークされていないことを確認した後にデータを読み出す構成とした。このことにより、不正な記録装置が、不正な記録データに対してデジタル署名を記録しないような攻撃を無力なものにしているとともに、不正な装置で記録されたデータを正当な装置で再生しないようにすることで、不正な装置のシステムからの排除をより強力に行っている。

【0229】

〔記録処理におけるコピー制御〕

さて、コンテンツの著作権者等の利益を保護するには、ライセンスを受けた装置において、コンテンツのコピーを制御する必要がある。

【0230】

即ち、コンテンツを記録媒体に記録する場合には、そのコンテンツが、コピー

しても良いもの（コピー可能）かどうかを調査し、コピーして良いコンテンツだけを記録するようにする必要がある。また、記録媒体に記録されたコンテンツを再生して出力する場合には、その出力するコンテンツが、後で、違法コピーされないようにする必要がある。

【0231】

そこで、そのようなコンテンツのコピー制御を行いながら、コンテンツの記録再生を行う場合の図1の記録再生装置の処理について、図33および図34のフローチャートを参照して説明する。

【0232】

まず、外部からのデジタル信号のコンテンツを、記録媒体に記録する場合においては、図33（A）のフローチャートにしたがった記録処理が行われる。図33（A）の処理について説明する。図1の記録再生器100を例として説明する。デジタル信号のコンテンツ（デジタルコンテンツ）が、例えば、IEEE1394シリアルバス等を介して、入出力I/F120に供給されると、ステップS701において、入出力I/F120は、そのデジタルコンテンツを受信し、ステップS702に進む。

【0233】

ステップS702では、入出力I/F120は、受信したデジタルコンテンツが、コピー可能であるかどうかを判定する。即ち、例えば、入出力I/F120が受信したコンテンツが暗号化されていない場合（例えば、上述のDTCPを使用せずに、平文のコンテンツが、入出力I/F120に供給された場合）には、そのコンテンツは、コピー可能であると判定される。

【0234】

また、記録再生装置100がDTCPに準拠している装置であるとし、DTCPに従って処理を実行するものとする。DTCPでは、コピーを制御するためのコピー制御情報としての2ビットのEMI (Encryption Mode Indicator)が規定されている。EMIが00B（Bは、その前の値が2進数であることを表す）である場合は、コンテンツがコピーフリーのもの(Copy-freely)であることを表し、EMIが01Bである場合には、コンテンツが、それ以上のコピーをすること

ができないもの(No-more-copies)であることを表す。さらに、EMIが10Bである場合は、コンテンツが、1度だけコピーして良いもの(Copy-one-generation)であることを表し、EMIが11Bである場合には、コンテンツが、コピーが禁止されているもの(Copy-never)であることを表す。

【0235】

記録再生装置100の入出力I/F120に供給される信号にEMIが含まれ、そのEMIが、Copy-freelyやCopy-one-generationであるときには、コンテンツはコピー可能であると判定される。また、EMIが、No-more-copiesやCopy-neverであるときには、コンテンツはコピー可能でないと判定される。

【0236】

ステップS702において、コンテンツがコピー可能でないと判定された場合、ステップS703～S705をスキップして、記録処理を終了する。従って、この場合には、コンテンツは、記録媒体10に記録されない。

【0237】

また、ステップS702において、コンテンツがコピー可能であると判定された場合、ステップS703に進み、以下、ステップS703～S705において、図3(A)のステップS12、S13、S14における処理と同様の処理が行われる。すなわち、TS処理手段300によるトランスポートパケットに対するATS付加、暗号処理手段150における暗号化処理が実行され、その結果得られる暗号化コンテンツを、記録媒体195に記録して、記録処理を終了する。

【0238】

なお、EMIは、入出力I/F120に供給されるデジタル信号に含まれるものであり、デジタルコンテンツが記録される場合には、そのデジタルコンテンツとともに、EMI、あるいは、EMIと同様にコピー制御状態を表す情報(例えば、DTCFにおけるembedded CCIなど)も記録される。

【0239】

この際、一般的には、Copy-One-Generationを表す情報は、それ以上のコピーを許さないよう、No-more-copiesに変換されて記録される。

【0240】

本発明の記録再生装置では、このEMIやembedded CCIなどのコピー制御情報を、TSパケットに付加する形で記録する。即ち、図10の例2や例3のように、ATSを24ビットないし30ビット分と、コピー制御情報を加えた32ビットを図5に示すように各TSパケットに付加する。

【0241】

外部からのアナログ信号のコンテンツを、記録媒体に記録する場合においては、図33(B)のフローチャートにしたがった記録処理が行われる。図33(B)の処理について説明する。アナログ信号のコンテンツ(アナログコンテンツ)が、入出力I/F140に供給されると、入出力I/F140は、ステップS711において、そのアナログコンテンツを受信し、ステップS712に進み、受信したアナログコンテンツが、コピー可能であるかどうかを判定する。

【0242】

ここで、ステップS712の判定処理は、例えば、入出力I/F140で受信した信号に、マクロビジョン(Macrovision)信号や、CGMS-A(Copy Generation Management System-Analog)信号が含まれるかどうかに基づいて行われる。即ち、マクロビジョン信号は、VHS方式のビデオカセットテープに記録すると、ノイズとなるような信号であり、これが、入出力I/F140で受信した信号に含まれる場合には、アナログコンテンツは、コピー可能でないと判定される。

【0243】

また、例えば、CGMS-A信号は、デジタル信号のコピー制御に用いられるCGMS信号を、アナログ信号のコピー制御に適用した信号で、コンテンツがコピーフリーのもの(Copy-freely)、1度だけコピーして良いもの(Copy-one-generation)、またはコピーが禁止されているもの(Copy-never)のうちのいずれであるかを表す。

【0244】

従って、CGMS-A信号が、入出力I/F140で受信した信号に含まれ、かつ、そのCGMS-A信号が、Copy-freelyやCopy-one-generationを表している場合には、アナログコンテンツは、コピー可能であると判定される。また、CGMS-A信号が、Copy-neverを表している場合には、アナログコンテンツは、

コピー可能でないと判定される。

【 0 2 4 5 】

さらに、例えば、マクロビジョン信号も、CGMS-A信号も、入出力I/F 4で受信した信号に含まれない場合には、アナログコンテンツは、コピー可能であると判定される。

【 0 2 4 6 】

ステップS 7 1 2において、アナログコンテンツがコピー可能でないと判定された場合、ステップS 7 1 3乃至S 7 1 7をスキップして、記録処理を終了する。従って、この場合には、コンテンツは、記録媒体10に記録されない。

【 0 2 4 7 】

また、ステップS 7 1 2において、アナログコンテンツがコピー可能であると判定された場合、ステップS 7 1 3に進み、以下、ステップS 7 1 3乃至S 7 1 7において、図3 (B)のステップS 2 2乃至S 2 6における処理と同様の処理が行われ、これにより、コンテンツがデジタル変換、MPEG符号化、TS処理、暗号化処理がなされて記録媒体に記録され、記録処理を終了する。

【 0 2 4 8 】

なお、入出力I/F 1 4 0で受信したアナログ信号に、CGMS-A信号が含まれている場合に、アナログコンテンツを記録媒体に記録するときには、そのCGMS-A信号も、記録媒体に記録される。即ち、図10で示したCCIもしくはその他の情報の部分に、この信号が記録される。この際、一般的には、Copy-0 ne-Generationを表す情報は、それ以上のコピーを許さないよう、No-more-copiesに変換されて記録される。ただし、システムにおいてたとえば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」などのルールが決められている場合は、この限りではない。

【 0 2 4 9 】

〔再生処理におけるコピー制御〕

次に、記録媒体に記録されたコンテンツを再生して、ディジタルコンテンツとして外部に出力する場合においては、図34 (A)のフローチャートにしたがった再生処理が行われる。図34 (A)の処理について説明する。まず最初に、ス

ステップ S 8 0 1、S 8 0 2、S 8 0 3において、図 4 (A) のステップ S 3 1、S 3 2、S 3 3における処理と同様の処理が行われ、これにより、記録媒体から読み出された暗号化コンテンツが暗号処理手段 1 5 0において復号処理がなされ、T S 処理がなされる。各処理が実行されたデジタルコンテンツは、バス 1 1 0を介して、入出力 I / F 1 2 0に供給される。

【 0 2 5 0 】

入出力 I / F 1 2 0は、ステップ S 8 0 4において、そこに供給されるデジタルコンテンツが、後でコピー可能なものかどうかを判定する。即ち、例えば、入出力 I / F 1 2 0に供給されるデジタルコンテンツに E M I、あるいは、E M Iと同様にコピー制御状態を表す情報（コピー制御情報）が含まれない場合には、そのコンテンツは、後でコピー可能なものであると判定される。

【 0 2 5 1 】

また、例えば、入出力 I / F 1 2 0に供給されるデジタルコンテンツに E M Iが含まれる場合、従って、コンテンツの記録時に、D T C Pの規格にしたがって、E M Iが記録された場合には、その E M I（記録された E M I (Recorded E M I)）が、Copy-freelyであるときには、デジタルコンテンツは、後でコピー可能なものであると判定される。また、E M Iが、No-more-copiesであるときには、コンテンツは、後でコピー可能なものでないと判定される。

【 0 2 5 2 】

なお、一般的には、記録された E M Iが、Copy-one-generationやCopy-neverであることはない。Copy-one-generationの E M Iは記録時にNo-more-copiesに変換され、また、Copy-neverの E M Iを持つデジタルコンテンツは、記録媒体に記録されないからである。ただし、システムにおいてたとえば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」などのルールが決められている場合は、この限りではない。

【 0 2 5 3 】

ステップ S 8 0 4において、コンテンツが、後でコピー可能なものであると判定された場合、ステップ S 8 0 5に進み、入出力 I / F 1 2 0は、そのディジタ

ルコンテンツを、外部に出力し、再生処理を終了する。

【 0 2 5 4 】

また、ステップ S 8 0 4 において、コンテンツが、後でコピー可能なものでないと判定された場合、ステップ S 8 0 6 に進み、入出力 I / F 1 2 0 は、例えば、DTCP の規格等にしながら、デジタルコンテンツを、そのデジタルコンテンツが後でコピーされないような形で外部に出力し、再生処理を終了する。

【 0 2 5 5 】

即ち、例えば、上述のように、記録された EMI が、No-more-copies である場合（もしくは、システムにおいてたとえば「Copy-one-generation のコピー制御情報は、No-more-copies に変換せずに記録するが、No-more-copies として扱う」というルールが決められていて、その条件下で記録された EMI が Copy-one-generation である場合）には、コンテンツは、それ以上のコピーは許されない。

【 0 2 5 6 】

このため、入出力 I / F 1 2 0 は、DTCP の規格にしながら、相手の装置との間で認証を相互に行い、相手が正当な装置である場合（ここでは、DTCP の規格に準拠した装置である場合）には、デジタルコンテンツを暗号化して、外部に出力する。

【 0 2 5 7 】

次に、記録媒体に記録されたコンテンツを再生して、アナログコンテンツとして外部に出力する場合においては、図 3 4 （B）のフローチャートにしたがった再生処理が行われる。図 3 4 （B）の処理について説明する。ステップ S 8 1 1 乃至 S 8 1 5 において、図 4 （B）のステップ S 4 1 乃至 S 4 5 における処理と同様の処理が行われる。すなわち、暗号化コンテンツの読み出し、復号処理、TS 処理、MPEG デコード、D / A 変換が実行される。これにより得られるアナログコンテンツは、入出力 I / F 1 4 0 で受信される。

【 0 2 5 8 】

入出力 I / F 1 4 0 は、ステップ S 8 1 6 において、そこに供給されるコンテンツが、後でコピー可能なものかどうかを判定する。即ち、例えば、記録されていたコンテンツに EMI などのコピー制御情報がいっしょに記録されていない場

合には、そのコンテンツは、後でコピー可能なものであると判定される。

【0259】

また、コンテンツの記録時に、例えばDTCPの規格にしたがって、EMIまたはコピー制御情報が記録された場合には、その情報が、Copy-freelyであるときには、コンテンツは、後でコピー可能なものであると判定される。

【0260】

また、EMIまたはコピー制御情報が、No-more-copiesである場合、もしくは、システムにおいてたとえば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」というルールが決められていて、その条件下で記録されたEMIまたはコピー制御情報がCopy-one-generationである場合には、コンテンツは、後でコピー可能なものでないと判定される。

【0261】

さらに、例えば、入出力I/F140に供給されるアナログコンテンツにCGMS-A信号が含まれる場合、従って、コンテンツの記録時に、そのコンテンツとともにCGMS-A信号が記録された場合には、そのCGMS-A信号が、Copy-freelyであるときには、アナログコンテンツは、後でコピー可能なものであると判定される。また、CGMS-A信号が、Copy-neverであるときには、アナログコンテンツは、後でコピー可能なものでないと判定される。

【0262】

ステップS816において、コンテンツが、後でコピー可能であると判定された場合、ステップS817に進み、入出力I/F140は、そこに供給されたアナログ信号を、そのまま外部に出力し、再生処理を終了する。

【0263】

また、ステップS816において、コンテンツが、後でコピー可能でないと判定された場合、ステップS818に進み、入出力I/F140は、アナログコンテンツを、そのアナログコンテンツが後でコピーされないような形で外部に出力し、再生処理を終了する。

【0264】

即ち、例えば、上述のように、記録された E M I 等のコピー制御情報が、No-more-copiesである場合（もしくは、システムにおいてたとえば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」というルールが決められていて、その条件下で記録された E M I 等のコピー制御情報がCopy-one-generationである場合）には、コンテンツは、それ以上のコピーは許されない。

【 0 2 6 5 】

このため、入出力 I / F 1 4 0 は、アナログコンテンツを、それに、例えば、マクロビジョン信号や、Copy-neverを表す G C M S - A 信号を付加して、外部に出力する。また、例えば、記録された C G M S - A 信号が、Copy-neverである場合にも、コンテンツは、それ以上のコピーは許されない。このため、入出力 I / F 1 4 0 は、C G M S - A 信号をCopy-neverに変更して、アナログコンテンツとともに、外部に出力する。

【 0 2 6 6 】

以上のように、コンテンツのコピー制御を行いながら、コンテンツの記録再生を行うことにより、コンテンツに許された範囲外のコピー（違法コピー）が行われることを防止することが可能となる。

【 0 2 6 7 】

〔データ処理手段の構成〕

なお、上述した一連の処理は、ハードウェアにより行うことは勿論、ソフトウェアにより行うこともできる。即ち、例えば、暗号処理手段 1 5 0 は暗号化／復号 L S I として構成することも可能であるが、汎用のコンピュータや、1チップのマイクロコンピュータにプログラムを実行させることにより行う構成とすることも可能である。同様に T S 処理手段 3 0 0 も処理をソフトウェアによって実行することが可能である。一連の処理をソフトウェアによって行う場合には、そのソフトウェアを構成するプログラムが、汎用のコンピュータや1チップのマイクロコンピュータ等にインストールされる。図 3 5 は、上述した一連の処理を実行するプログラムがインストールされるコンピュータの一実施の形態の構成例を示している。

【 0 2 6 8 】

プログラムは、コンピュータに内蔵されている記録媒体としてのハードディスク 2 0 0 5 や ROM 2 0 0 3 に予め記録しておくことができる。あるいは、プログラムはフロッピーディスク、CD-ROM (Compact Disc Read Only Memory)、MO (Magneto optical) ディスク、DVD (Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体 2 0 1 0 に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体 2 0 1 0 は、いわゆるパッケージソフトウェアとして提供することができる。

【 0 2 6 9 】

なお、プログラムは、上述したようなリムーバブル記録媒体 2 0 1 0 からコンピュータにインストールする他、ダウンロードサイトから、デジタル衛星放送用の人工衛星を介して、コンピュータに無線で転送したり、LAN (Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを、通信部 2 0 0 8 で受信し、内蔵するハードディスク 2 0 0 5 にインストールすることができる。

【 0 2 7 0 】

コンピュータは、CPU (Central Processing Unit) 2 0 0 2 を内蔵している。CPU 2 0 0 2 には、バス 2 0 0 1 を介して、入出力インタフェース 2 0 1 1 が接続されており、CPU 2 0 0 2 は、入出力インタフェース 2 0 1 0 を介して、ユーザによって、キーボードやマウス等で構成される入力部 2 0 0 7 が操作されることにより指令が入力されると、それにしたがって、ROM (Read Only Memory) 2 0 0 3 に格納されているプログラムを実行する。

【 0 2 7 1 】

あるいは、CPU 2 0 0 2 は、ハードディスク 2 0 0 5 に格納されているプログラム、衛星若しくはネットワークから転送され、通信部 2 0 0 8 で受信されてハードディスク 2 0 0 5 にインストールされたプログラム、またはドライブ 2 0 0 9 に装着されたリムーバブル記録媒体 2 0 1 0 から読み出されてハードディスク 2 0 0 5 にインストールされたプログラムを、RAM (Random Access Memory)

2004にロードして実行する。

【0272】

これにより、CPU2002は、上述したフローチャートにしたがった処理、あるいは上述したブロック図の構成により行われる処理を行う。そして、CPU2002は、その処理結果を、必要に応じて、例えば、入出力インタフェース2011を介して、LCD(Liquid Crystal Display)やスピーカ等で構成される出力部2006から出力、あるいは、通信部2008から送信、さらには、ハードディスク2005に記録させる。

【0273】

ここで、本明細書において、コンピュータに各種の処理を行わせるためのプログラムを記述する処理ステップは、必ずしもフローチャートとして記載された順序に沿って時系列に処理する必要はなく、並列的あるいは個別に実行される処理（例えば、並列処理あるいはオブジェクトによる処理）も含むものである。

【0274】

また、プログラムは、1のコンピュータにより処理されるものであっても良いし、複数のコンピュータによって分散処理されるものであっても良い。さらに、プログラムは、遠方のコンピュータに転送されて実行されるものであっても良い。

【0275】

なお、本実施の形態では、コンテンツの暗号化／復号を行うブロックを、1チップの暗号化／復号LSIで構成する例を中心として説明したが、コンテンツの暗号化／復号を行うブロックは、例えば、図1に示すCPU170が実行する1つのソフトウェアモジュールとして実現することも可能である。同様に、TS処理手段300の処理もCPU170が実行する1つのソフトウェアモジュールとして実現することが可能である。

【0276】

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであ

り、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【 0 2 7 7 】

【発明の効果】

以上、説明したように、本発明の構成によれば情報記録装置がデータを情報記録媒体に記録する際に自身のデジタル署名および公開鍵証明書をデータと共に記録する。このことにより、情報を記録する際には、必ず、どの記録装置が記録したかという証拠もデータと共に記録するようにした。情報再生装置は、コンテンツの復号処理以前に署名および公開鍵証明書の正当性を確認し、コンテンツ記録者を特定し、公開鍵証明書、デジタル署名の改竄の無いことを確認する。本構成により、不正な記録装置による記録コンテンツの利用（再生）の効率的排除が可能となる。また、不正に記録されたデータを含む記録媒体が流通したとしても、それをどの記録装置が記録したか特定できるので、システムからの排除が行える。

【図面の簡単な説明】

【図 1】

本発明の情報記録再生装置の構成例を示すブロック図である。

【図 2】

本発明の情報記録再生装置において適用される公開鍵証明書の例を示す図である。

【図 3】

本発明の情報記録再生装置のデータ記録処理フローを示す図である。

【図 4】

本発明の情報記録再生装置のデータ再生処理フローを示す図である。

【図 5】

本発明の情報記録再生装置において処理されるデータフォーマットを説明する図である。

【図 6】

本発明の情報記録再生装置におけるトランスポート・ストリーム（TS）処理手段の構成を示すブロック図である。

【図 7】

本発明の情報記録再生装置において処理されるトランスポート・ストリームの構成を説明する図である。

【図 8】

本発明の情報記録再生装置におけるトランスポート・ストリーム (TS) 処理手段の構成を示すブロック図である。

【図 9】

本発明の情報記録再生装置におけるトランスポート・ストリーム (TS) 処理手段の構成を示すブロック図である。

【図 10】

本発明の情報記録再生装置において処理されるブロックデータの付加情報としてのブロック・データの構成例を示す図である。

【図 11】

本発明の情報記録再生装置に対する EKB 配信処理について説明するツリー構成図である。

【図 12】

本発明の情報記録再生装置に対するキー配布に使用される EKB の例を示す図である。

【図 13】

本発明の情報記録再生装置におけるメディアキーの EKB を使用した配布例と復号処理例を示す図である。

【図 14】

本発明の情報記録再生装置におけるメディアキーを使用したデータ記録処理時の暗号化処理を説明するブロック図である。

【図 15】

本発明の情報記録再生装置において適用可能なディスク固有キーの生成例を説明する図である。

【図 16】

本発明の情報記録再生装置において、適用可能なタイトル固有キーの生成処理

例を示す図である。

【図 1 7】

本発明の情報記録再生装置において適用可能なブロック・キーの生成方法を説明する図である。

【図 1 8】

本発明の情報記録再生装置におけるデータ記録処理時の暗号化処理を説明するブロック図である。

【図 1 9】

本発明の情報記録再生装置において暗号化コンテンツに対する署名を生成してデータ記録を行なう処理を説明するフロー図である。

【図 2 0】

本発明の情報記録再生装置において記録される暗号化コンテンツと公開鍵証明書、署名等との対応を管理するテーブルの構成例を示す図である。

【図 2 1】

本発明の情報記録再生装置においてタイトルキーに対する署名を生成してデータ記録を行なう処理を説明するフロー図である。

【図 2 2】

本発明の情報記録再生装置におけるデータ再生処理時の復号処理を説明するブロック図である。

【図 2 3】

本発明の情報記録再生装置において利用されるリボケーションテーブルの構成例を示す図である。

【図 2 4】

本発明の情報記録再生装置において E K B 配信ツリーをリボークデバイスの検査に適用させる場合の処理を説明する図である。

【図 2 5】

本発明の情報記録再生装置において適用可能な有効化キーブロック（E K B）のフォーマット例を示す図である。

【図 2 6】

有効化キーブロック（E K B）のタグの構成を説明する図である。

【図 2 7】

リボークエンティティ判定のための E K B 追跡処理について説明する図（例 1）である。

【図 2 8】

リボークエンティティ判定のための E K B 追跡処理について説明する図（例 2）である。

【図 2 9】

リボークエンティティ判定のための E K B 追跡処理について説明するフロー図である。

【図 3 0】

本発明の情報記録再生装置において署名を検証してデータ再生を行なう処理を説明するフロー図である。

【図 3 1】

本発明の情報記録再生装置において暗号化コンテンツに対する署名を検証してデータ再生を行なう処理を説明するフロー図である。

【図 3 2】

本発明の情報記録再生装置においてタイトルキーに対する署名を検証してデータ再生を行なう処理を説明するフロー図である。

【図 3 3】

本発明の情報記録再生装置におけるデータ記録処理時のコピー制御処理を説明するフローチャートである。

【図 3 4】

本発明の情報記録再生装置におけるデータ再生処理時のコピー制御処理を説明するフローチャートである。

【図 3 5】

本発明の情報記録再生装置において、データ処理をソフトウェアによって実行する場合の処理手段構成を示したブロック図である。

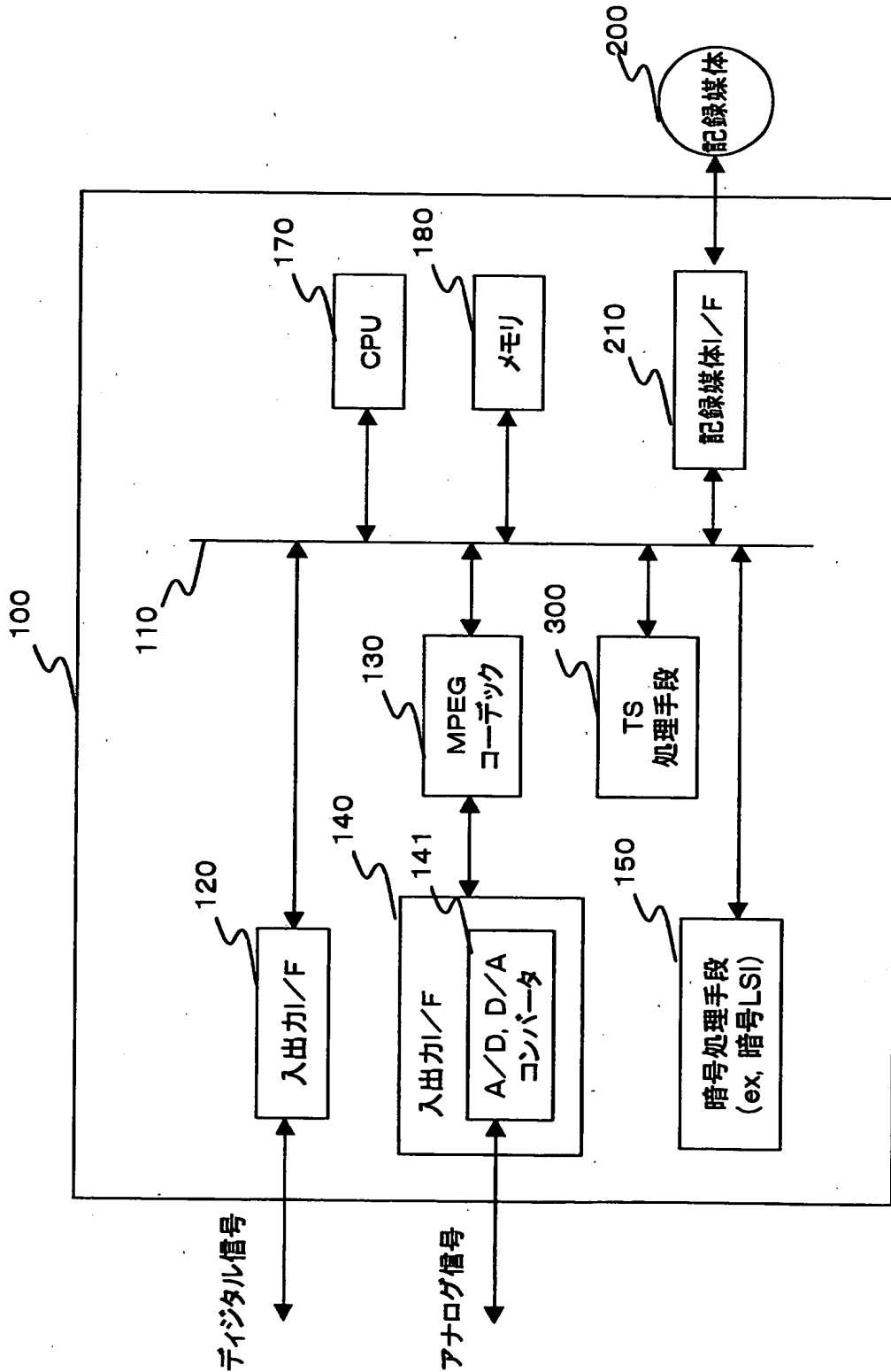
【符号の説明】

- 100 記録再生装置
- 110 バス
- 120 入出力 I/F
- 130 MPEGコーデック
- 140 入出力 I/F
- 141 A/D, D/Aコンバータ
- 150 暗号処理手段
- 160 ROM
- 170 CPU
- 180 メモリ
- 190 ドライブ
- 200 記録媒体
- 210 記録媒体 I/F
- 300 TS処理手段
- 600, 607 端子
- 602 ビットストリームパーサー
- 603 PLL
- 604 タイムスタンプ発生回路
- 605 ブロックシード付加回路
- 606 スムージングバッファ
- 800, 806 端子
- 801 ブロックシード分離回路
- 802 出力制御回路
- 803 比較器
- 804 タイミング発生回路
- 805 27MHzクロック
- 901, 904, 913 端子
- 902 MPEGビデオエンコーダ
- 903 ビデオストリームバッファ

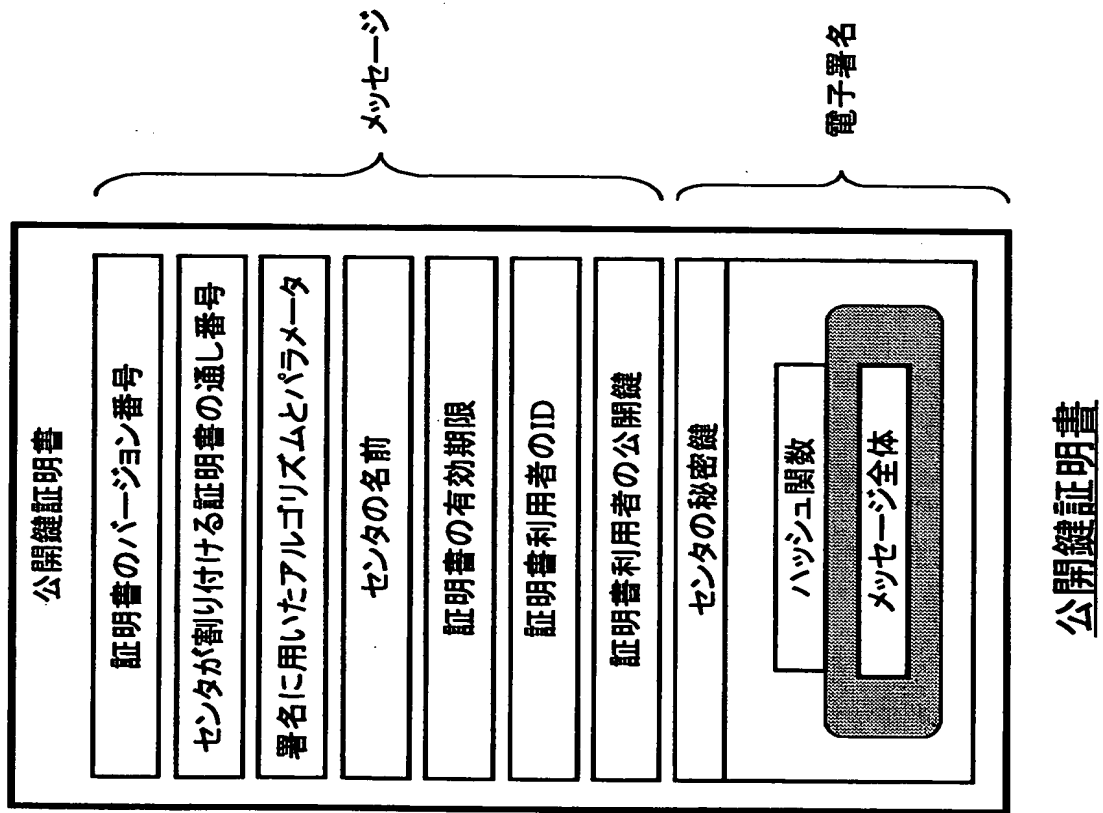
- 9 0 5 M P E Gオーディオエンコーダ
- 9 0 6 オーディオストリームバッファ
- 9 0 8 多重化スケジューラ
- 9 0 9 トランスポートパケット符号化器
- 9 1 0 到着タイムスタンプ計算手段
- 9 1 1 ブロックシード付加回路
- 9 1 2 スムージングバッファ
- 9 7 6 スイッチ
- 1 0 0 1 バージョン
- 1 0 0 2 デプス
- 1 0 0 3 データポインタ
- 1 0 0 4 タグポインタ
- 1 0 0 5 署名ポインタ
- 1 0 0 6 データ部
- 1 0 0 7 タグ部
- 1 0 0 8 署名
- 2 0 0 1 バス
- 2 0 0 2 C P U
- 2 0 0 3 R O M
- 2 0 0 4 R A M
- 2 0 0 5 ハードディスク
- 2 0 0 6 出力部
- 2 0 0 7 入力部
- 2 0 0 8 通信部
- 2 0 0 9 ドライブ
- 2 0 1 0 リムーバブル記録媒体
- 2 0 1 1 入出力インタフェース

【書類名】 図面

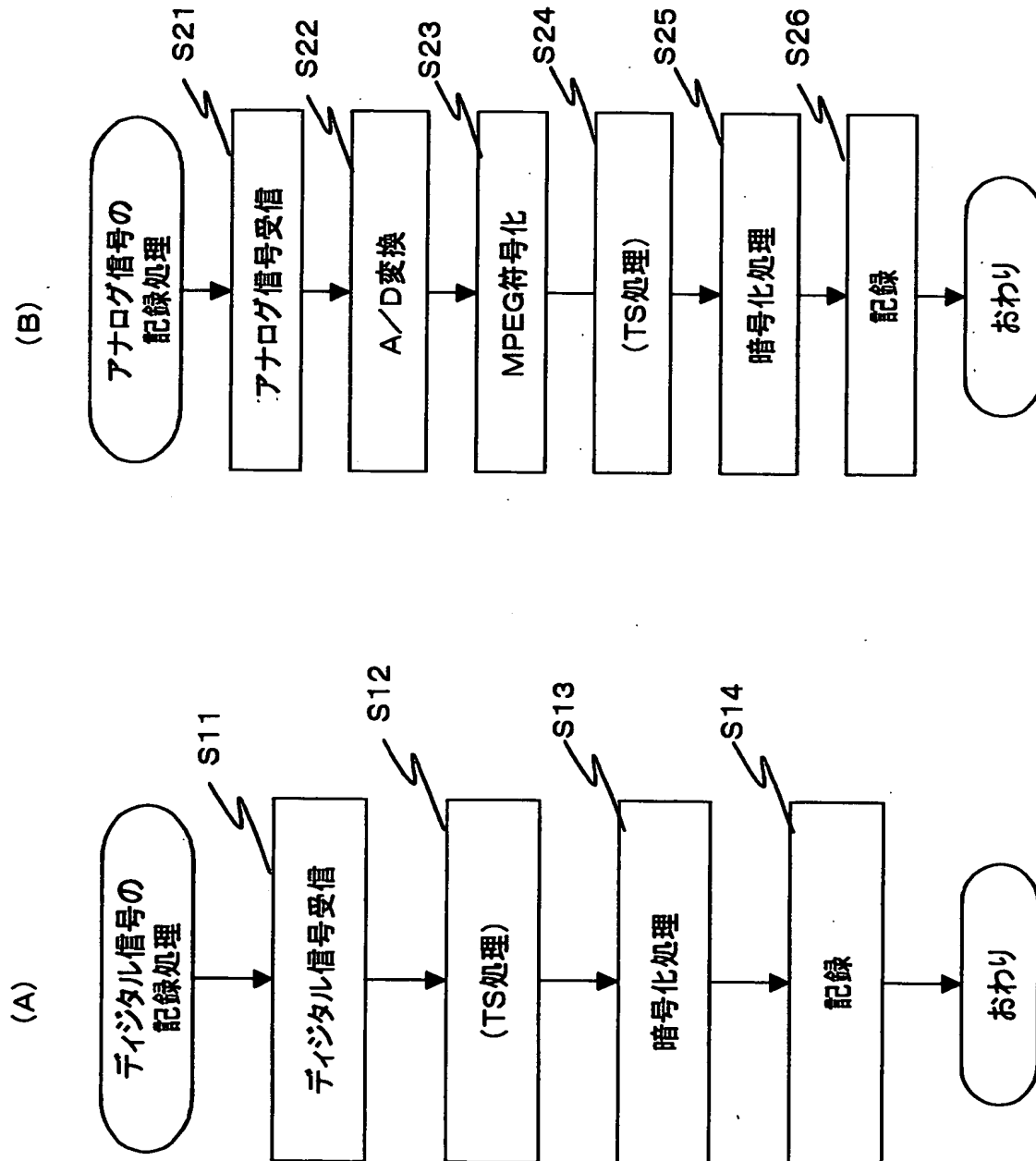
【図 1】



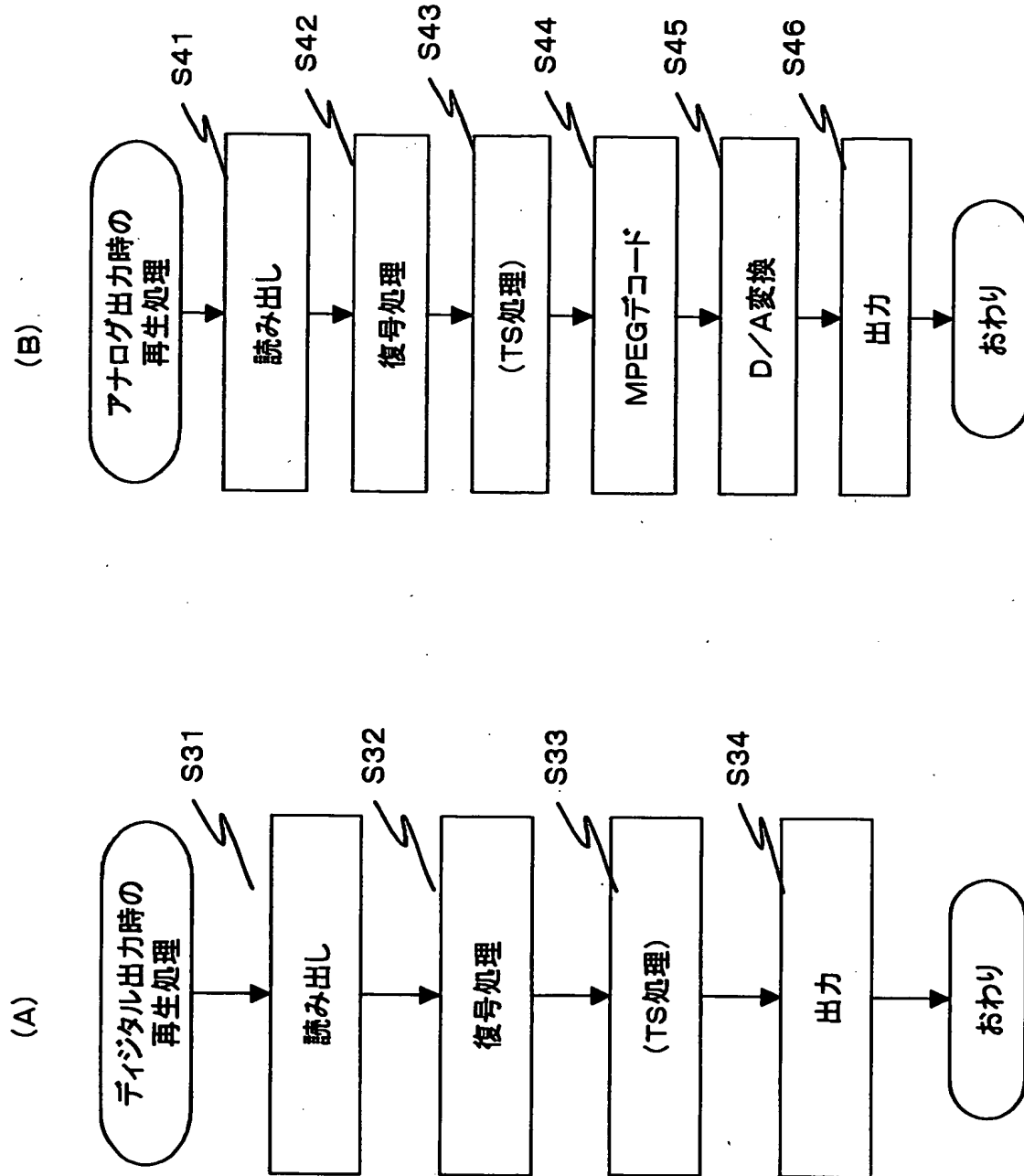
【図2】



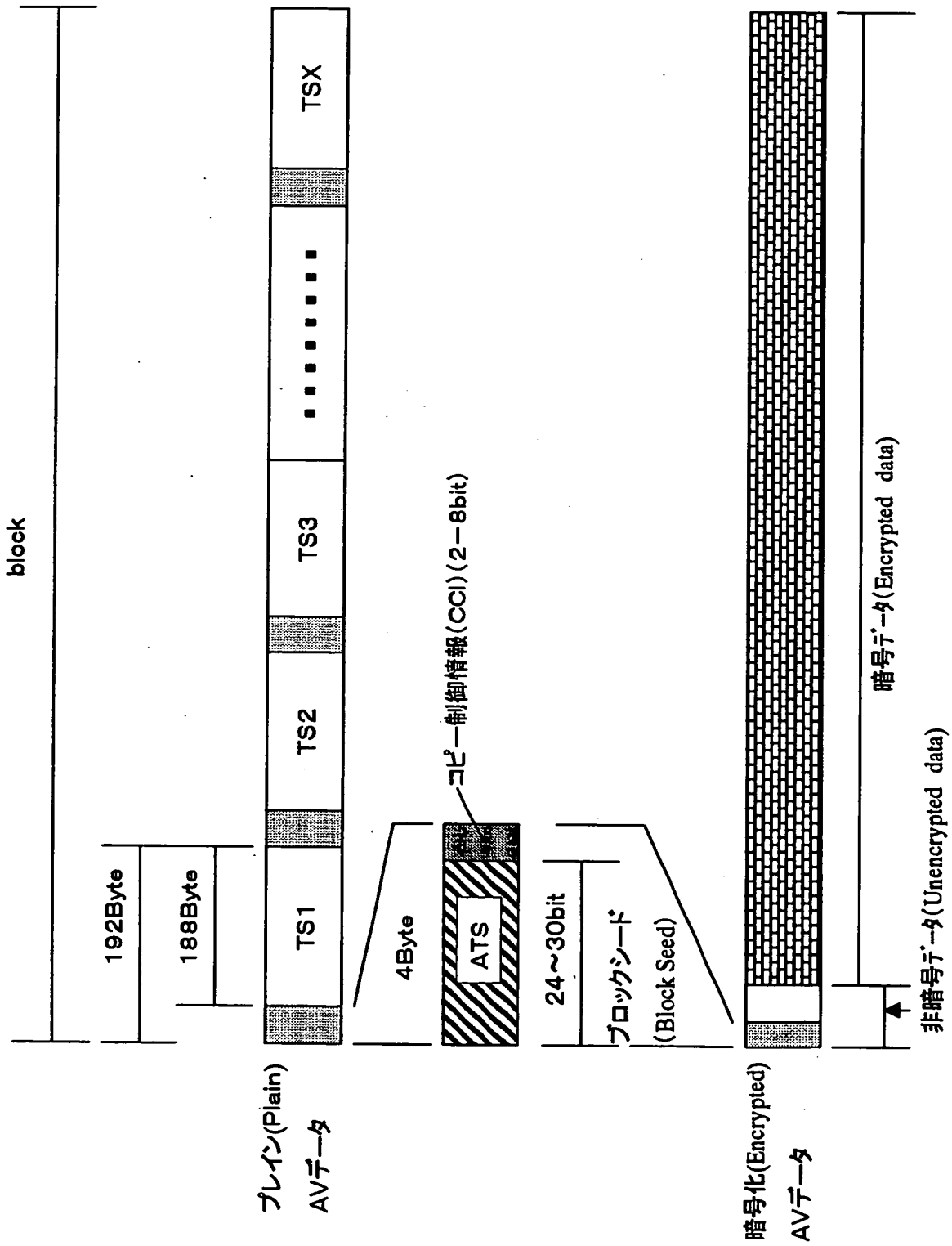
【図 3】



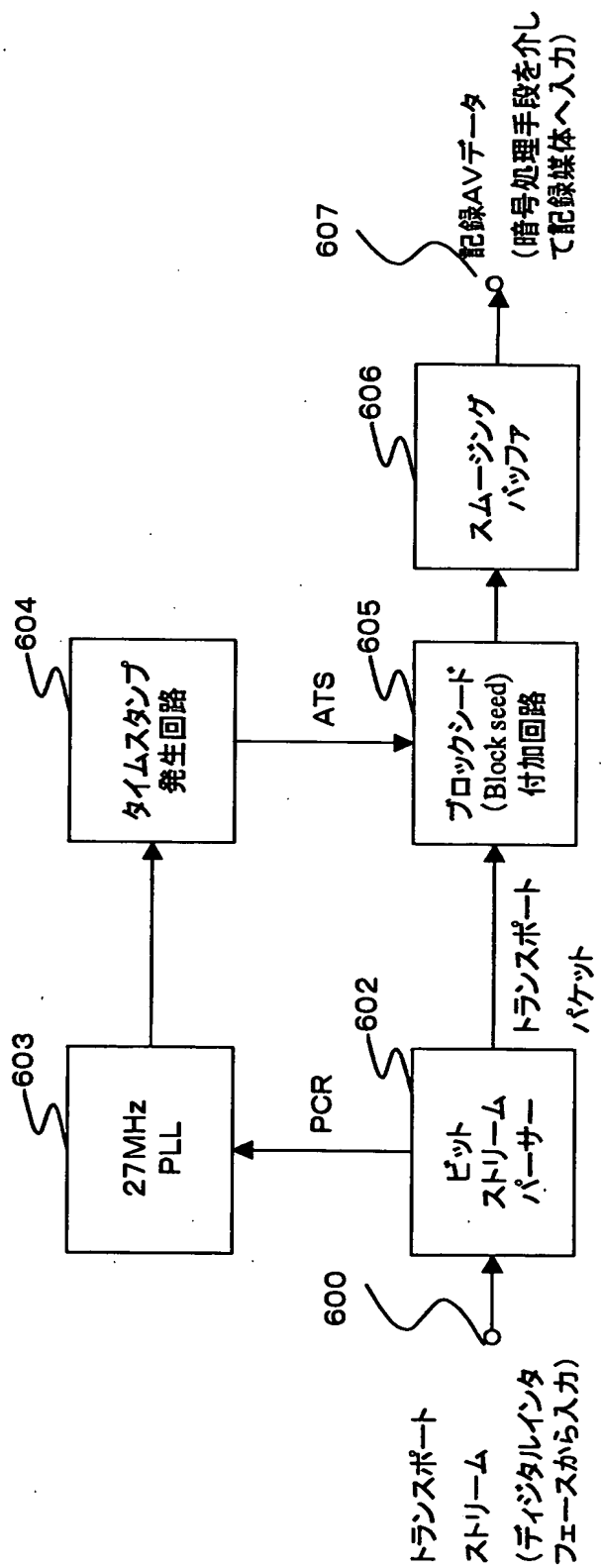
【図 4】



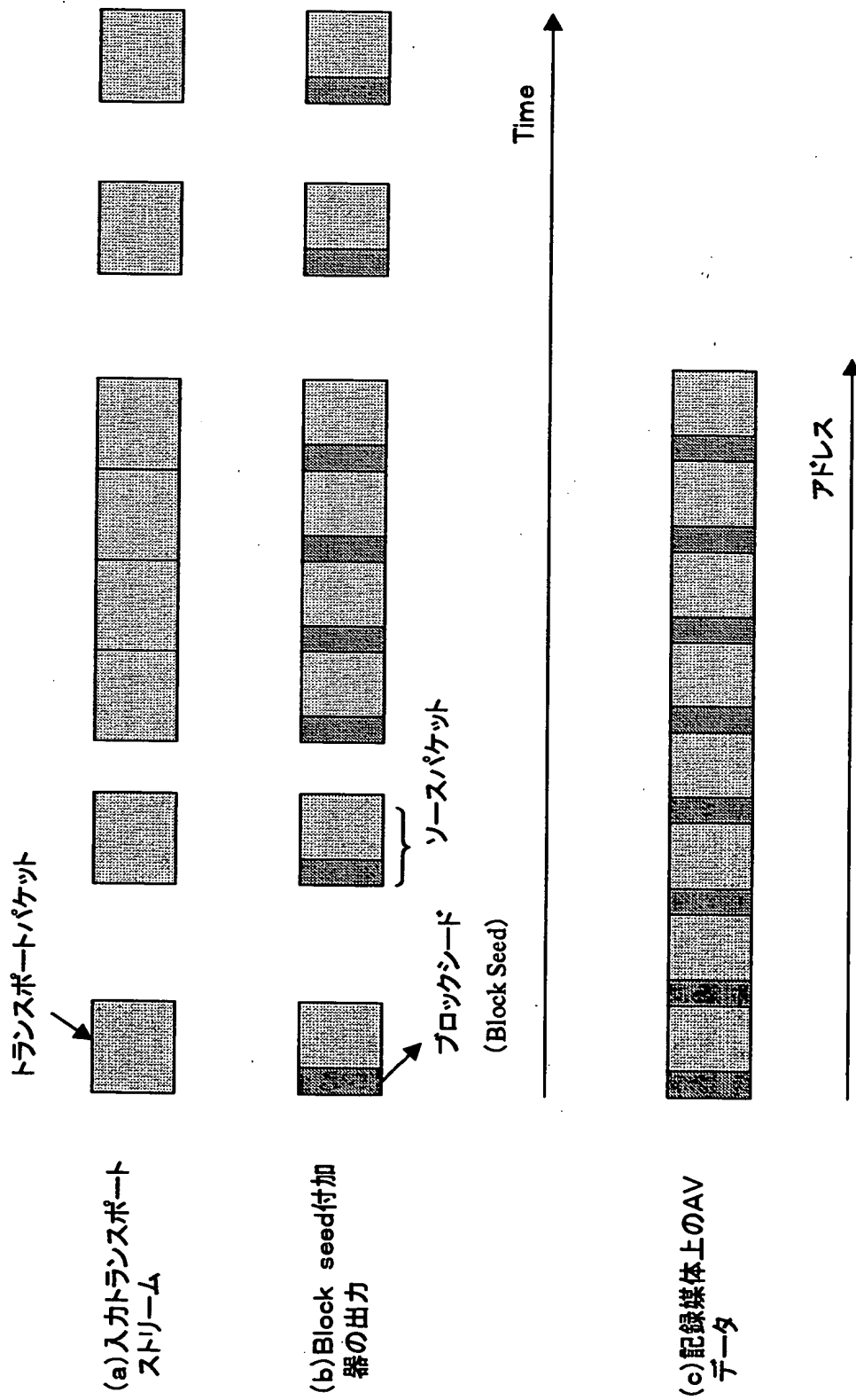
【図 5】



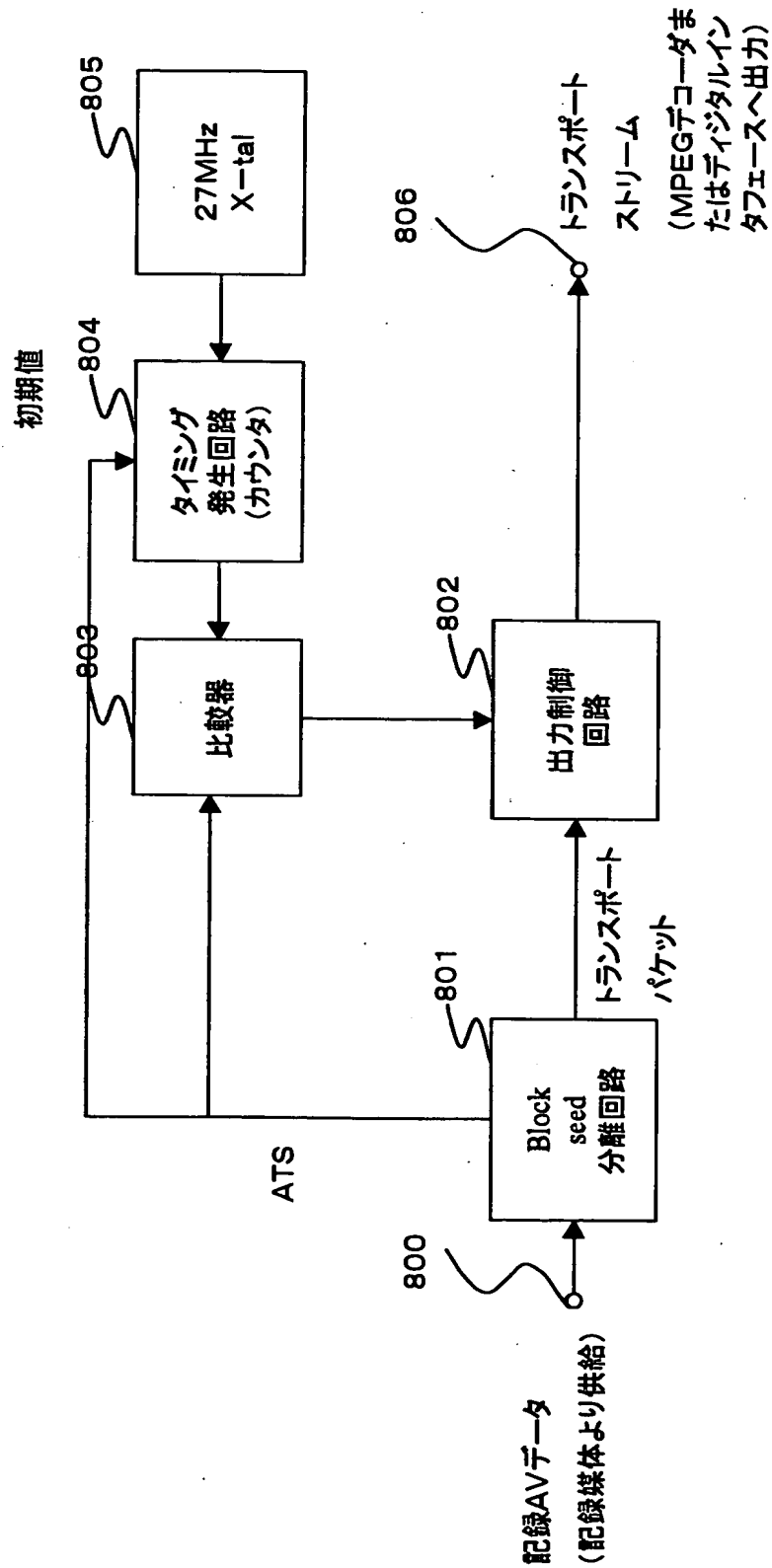
【図 6】



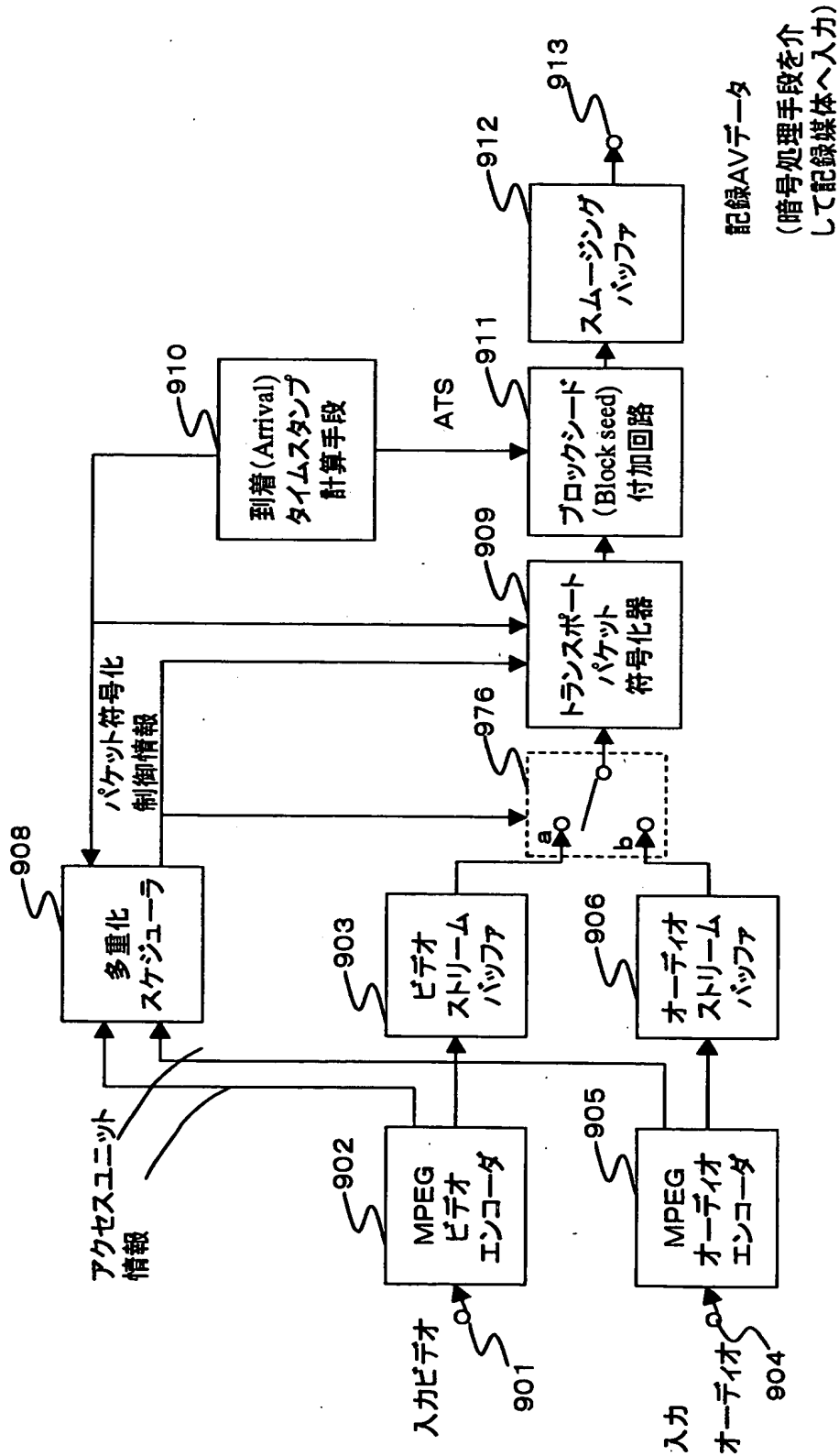
【図 7】



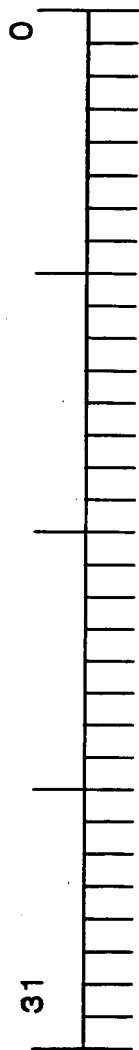
【図 8】



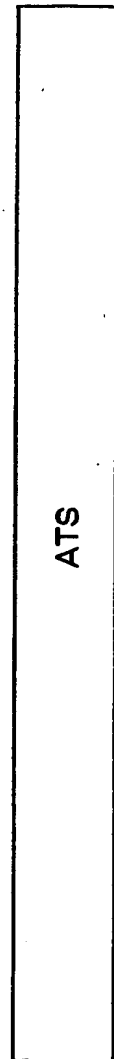
【図9】



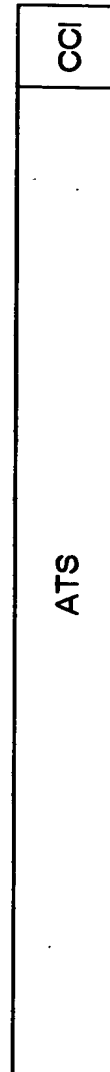
【図 10】



ブロックシード
(Block Seed)



例1
ATS 32bit

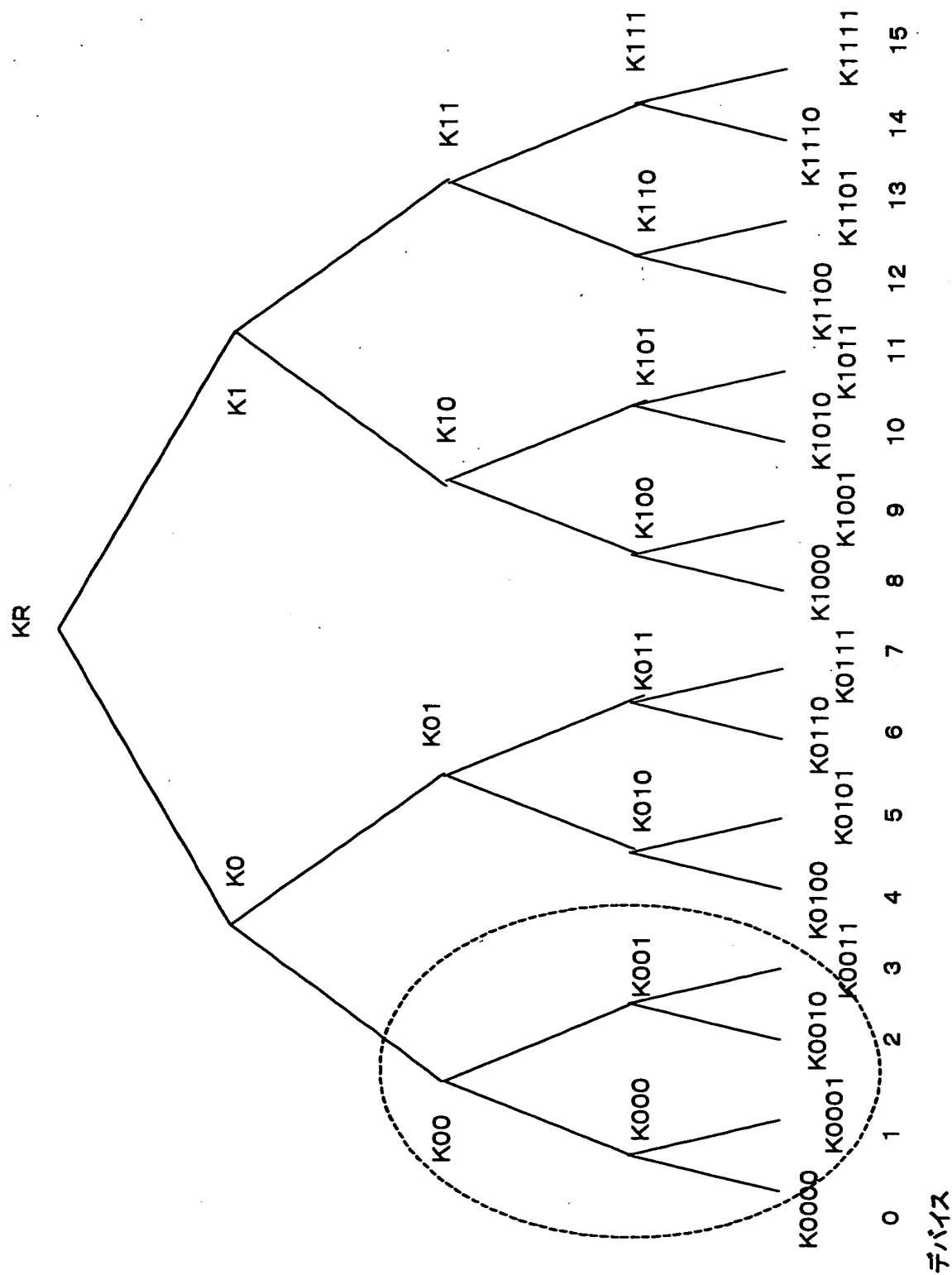


例2
ATS 30bit
CCI 2bit



例3
ATS 24bit
CCI 2bit
other info 6bit

【図11】



【図 12】

(A) 有効化キーブロック(EKB) 例1

デバイス0, 1, 2にt時点でのルートキー $K(t)R$ を送付

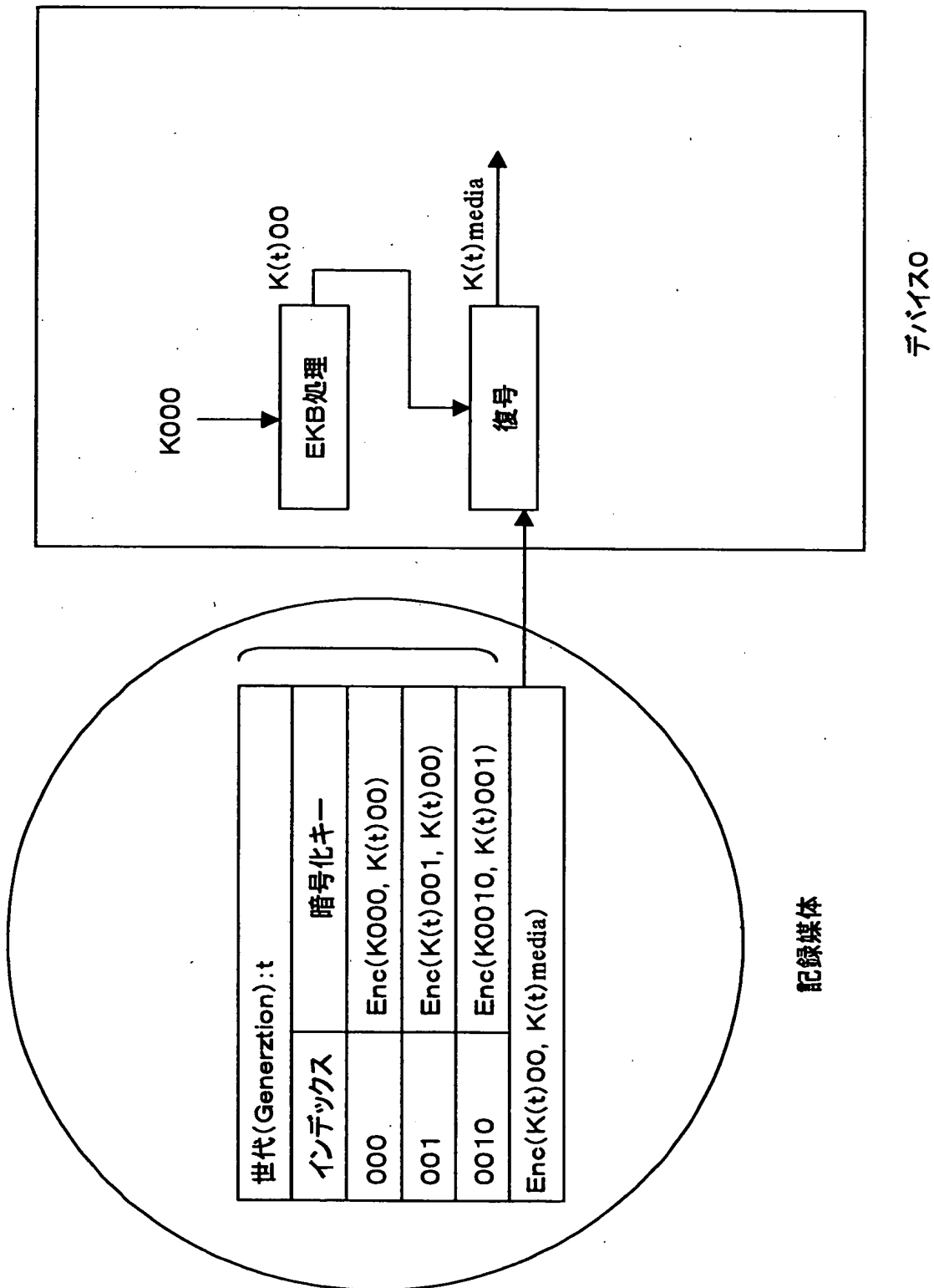
世代(Generztion):t	
インデックス	暗号化キー
0	$Enc(K(t)0, K(t)R)$
00	$Enc(K(t)00, K(t)0)$
000	$Enc(K000, K(t)00)$
001	$Enc(K(t)001, K(t)00)$
0010	$Enc(K0010, K(t)001)$

(B) 有効化キーブロック(EKB) 例2

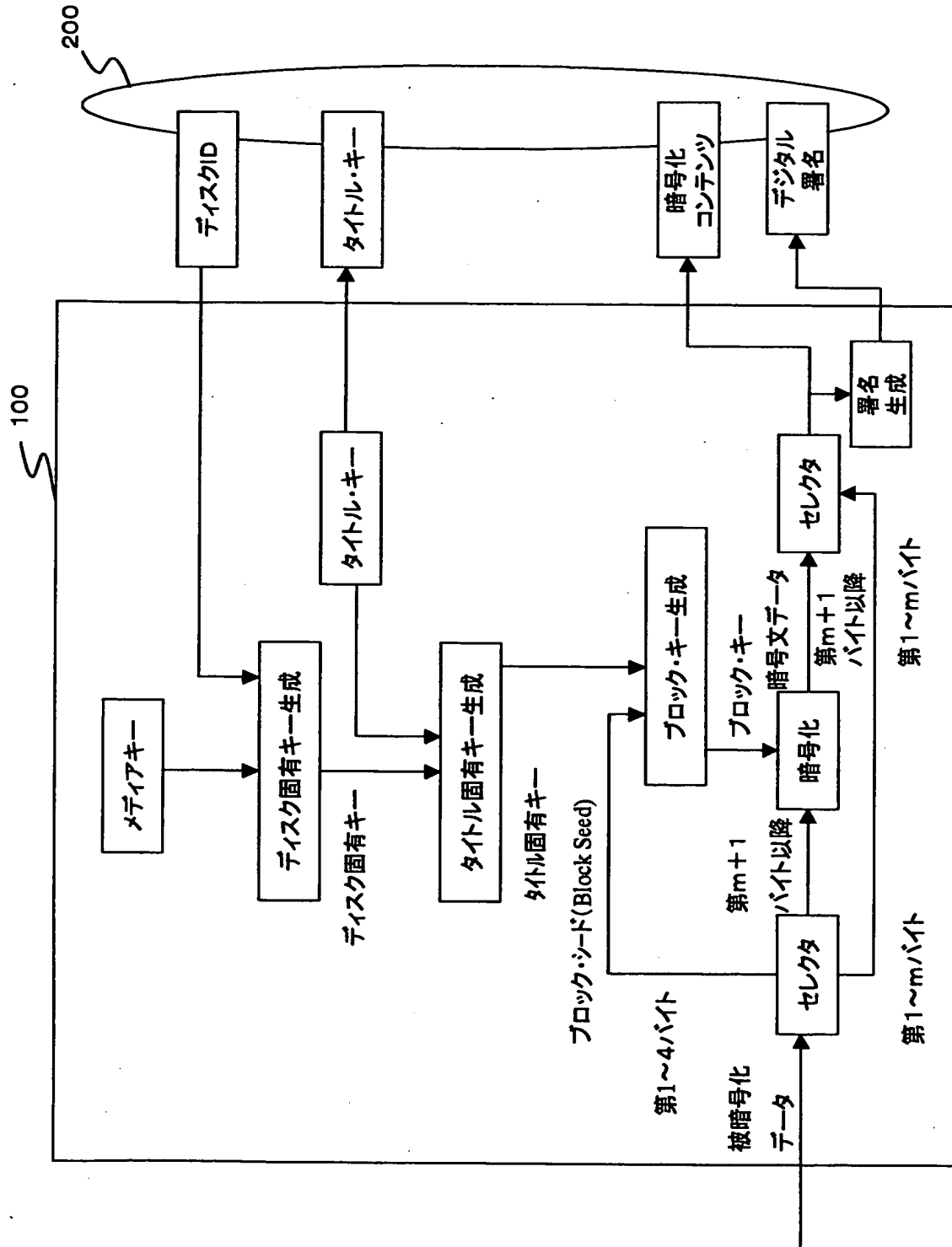
デバイス0, 1, 2にt時点でのルートキー $K(t)R$ を送付

世代(Generztion):t	
インデックス	暗号化キー
000	$Enc(K000, K(t)00)$
001	$Enc(K(t)001, K(t)00)$
0010	$Enc(K0010, K(t)001)$

【図 13】



【図14】



【図 1 5】

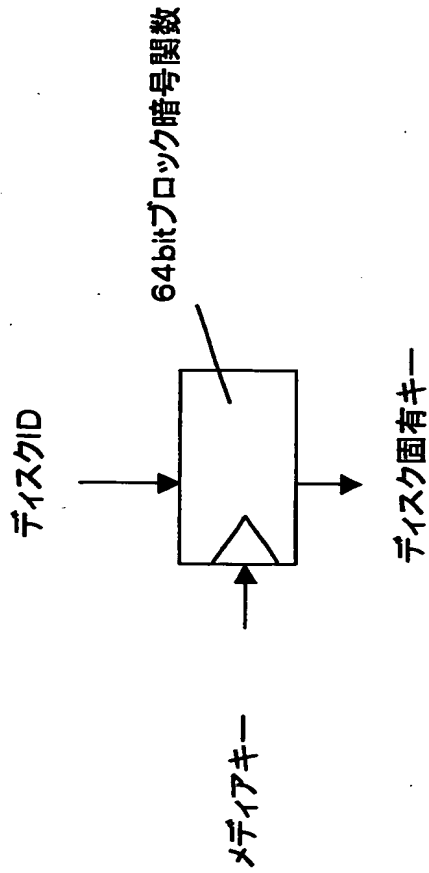
例 1

ディスク固有キー生成例

入力

メディアキー (64bit)

ディスクID (64bit)

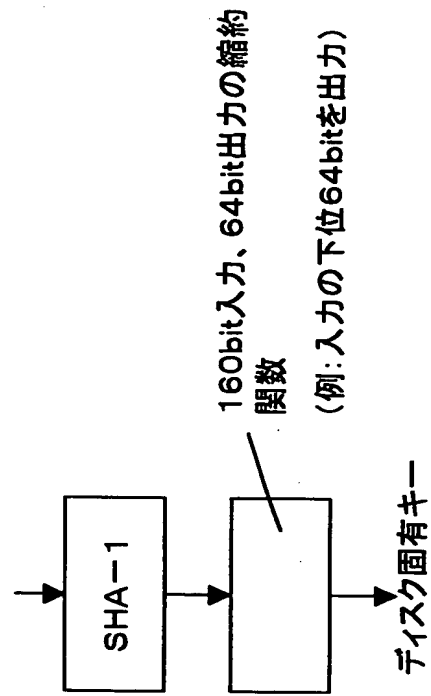


例 2

ディスク固有キー (64bit)

出力

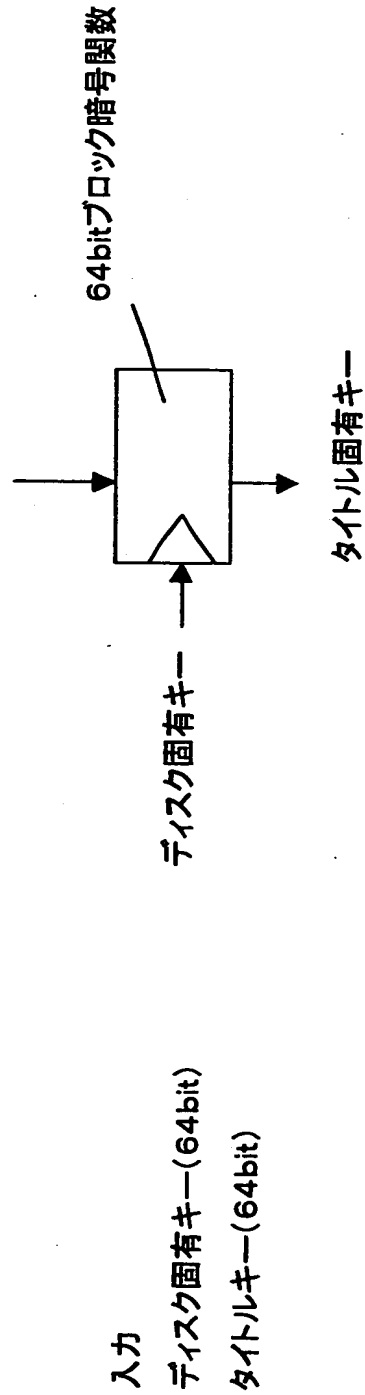
メディアキー || ディスクID



【図16】

例1

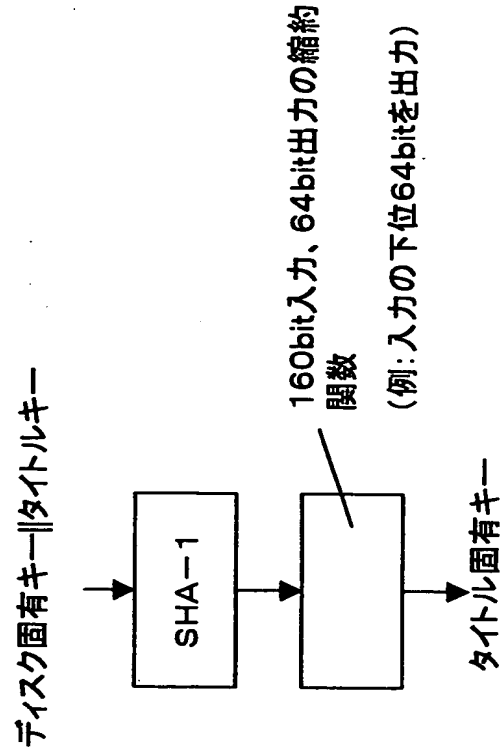
タイトル固有キー生成例



例2

出力

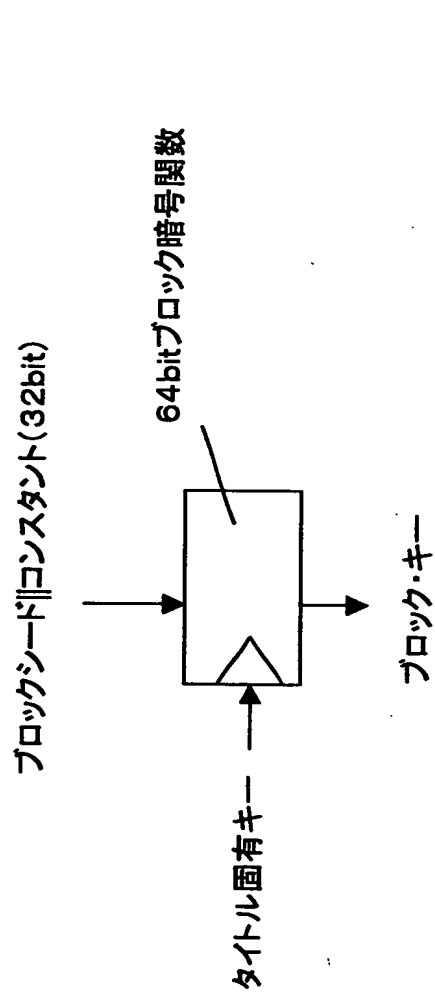
タイトル固有キー(64bit)



【図 1 7】

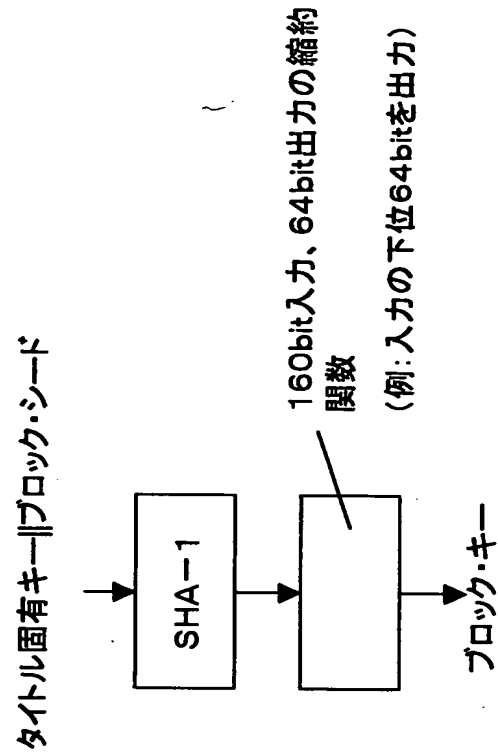
例 1

ブロックキー生成例
 入力
 ブロックシード(32bit)
 タイトル固有キー(64bit)

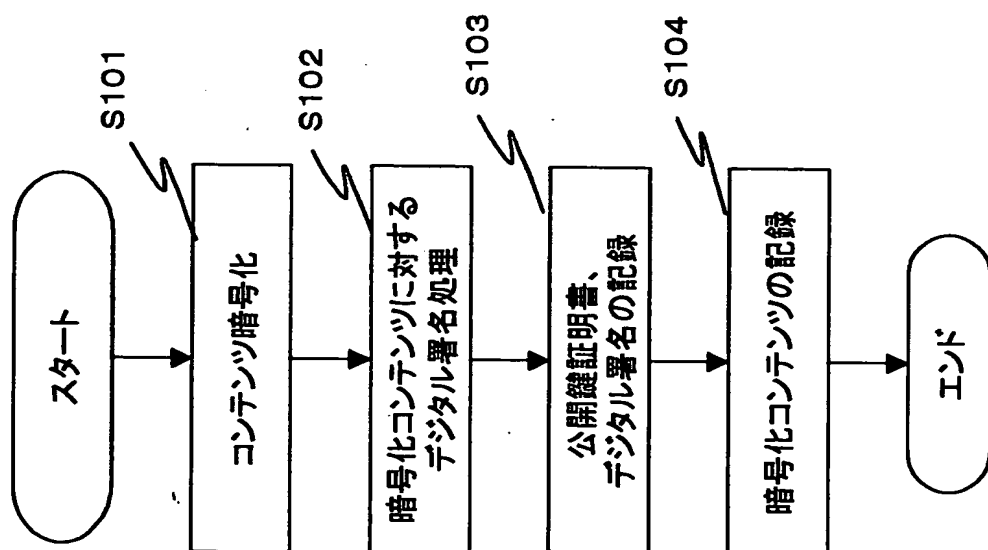


例 2

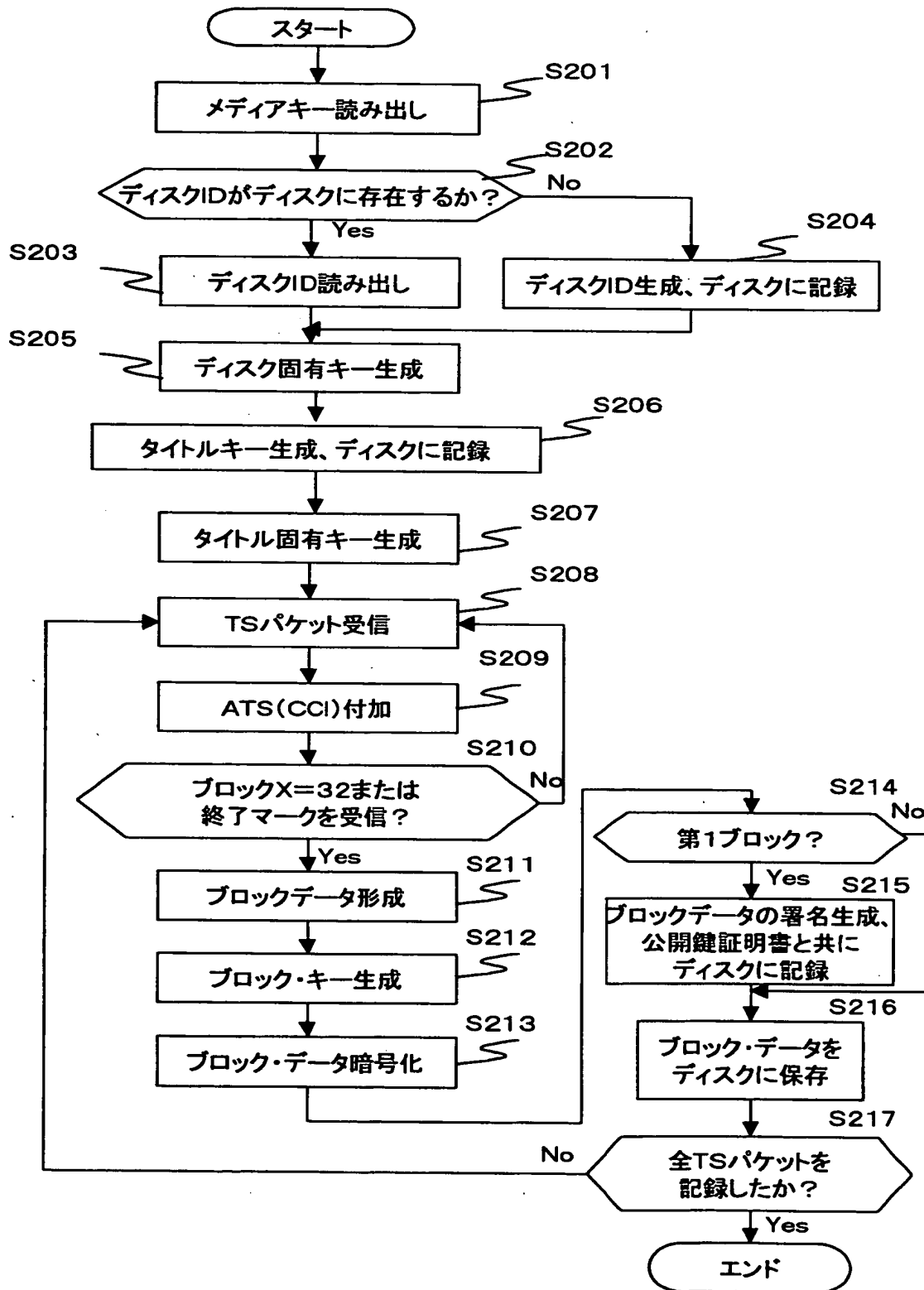
出力
 ブロック・キー(64bit)



【図 18】



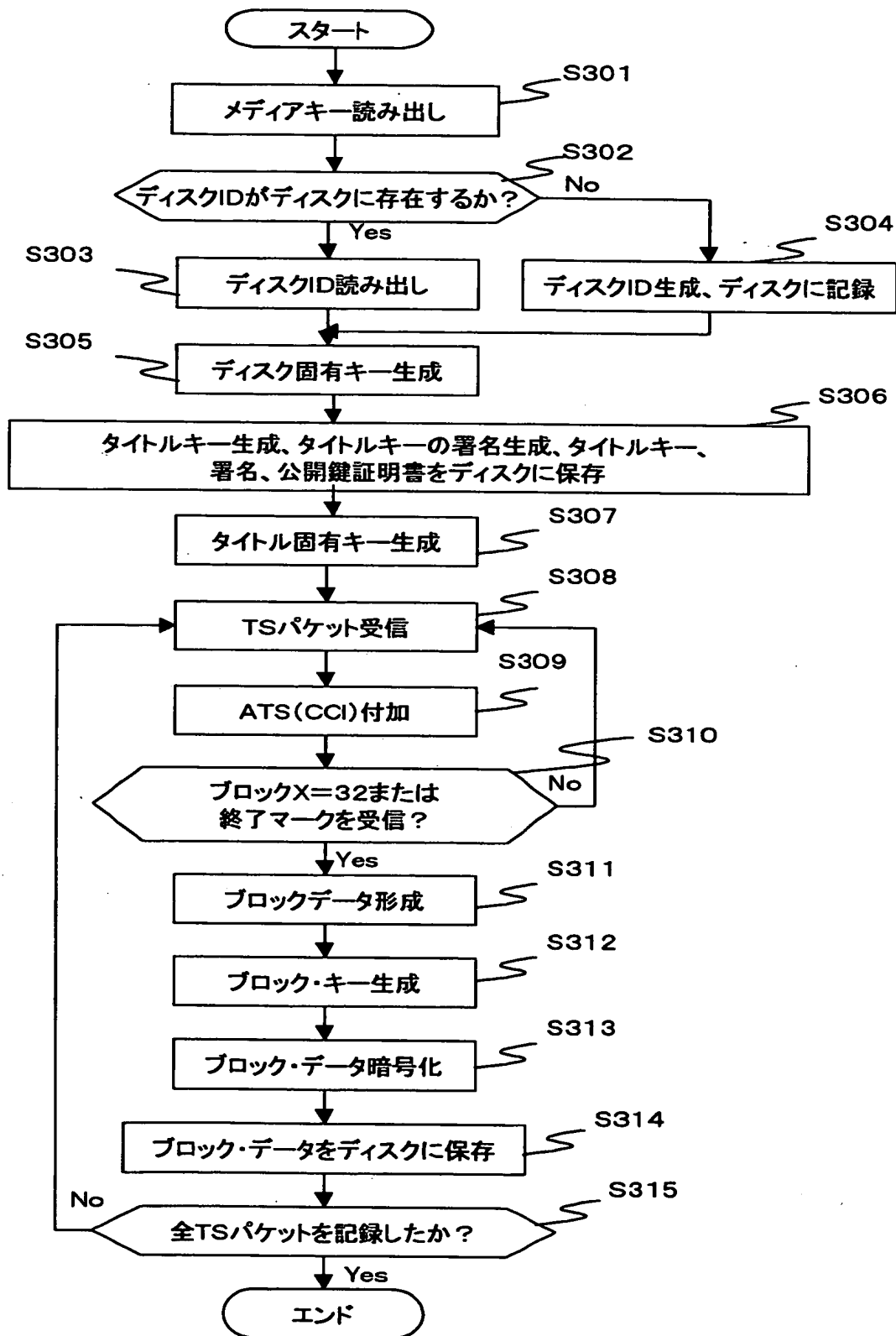
【図 19】



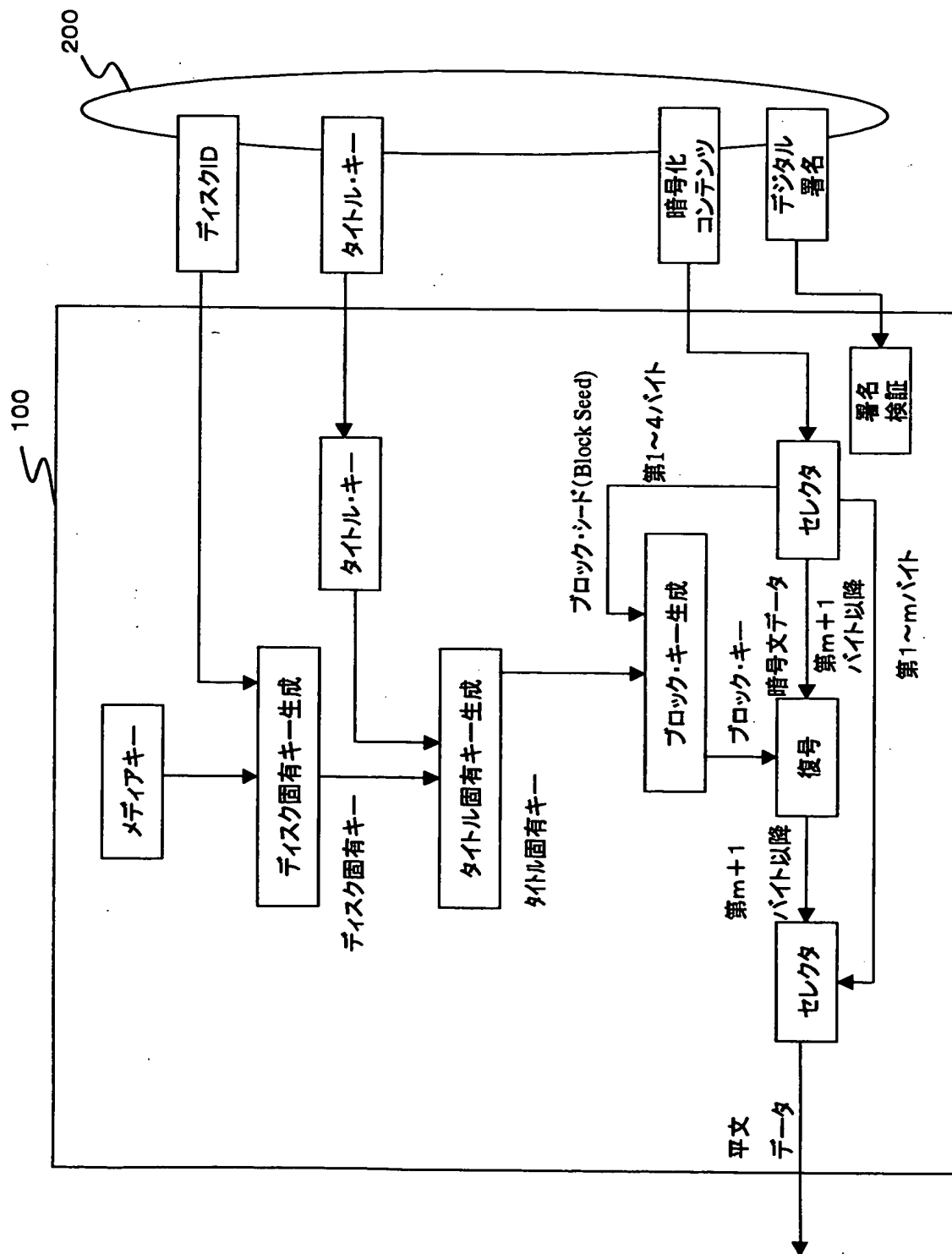
【図20】

ファイル1	コンテンツデータのアドレス
	タイトルキーのアドレス
	デジタル署名のアドレス
	公開鍵証明書のアドレス
	その他の情報
ファイル2	コンテンツデータのアドレス
	タイトルキーのアドレス
	デジタル署名のアドレス
	公開鍵証明書のアドレス
	その他の情報
：	：

【図 2 1】



【図 22】

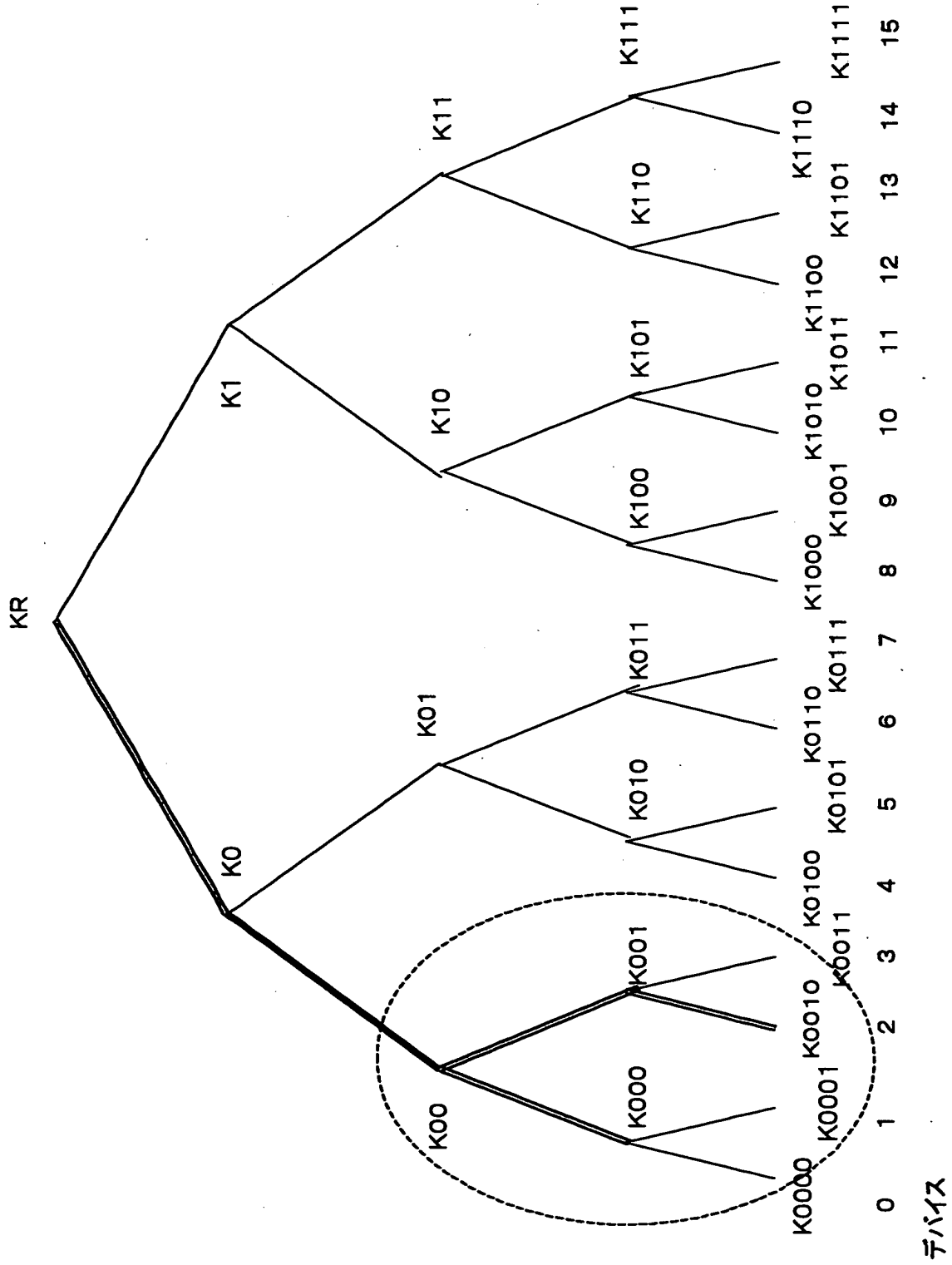


【図 2 3】

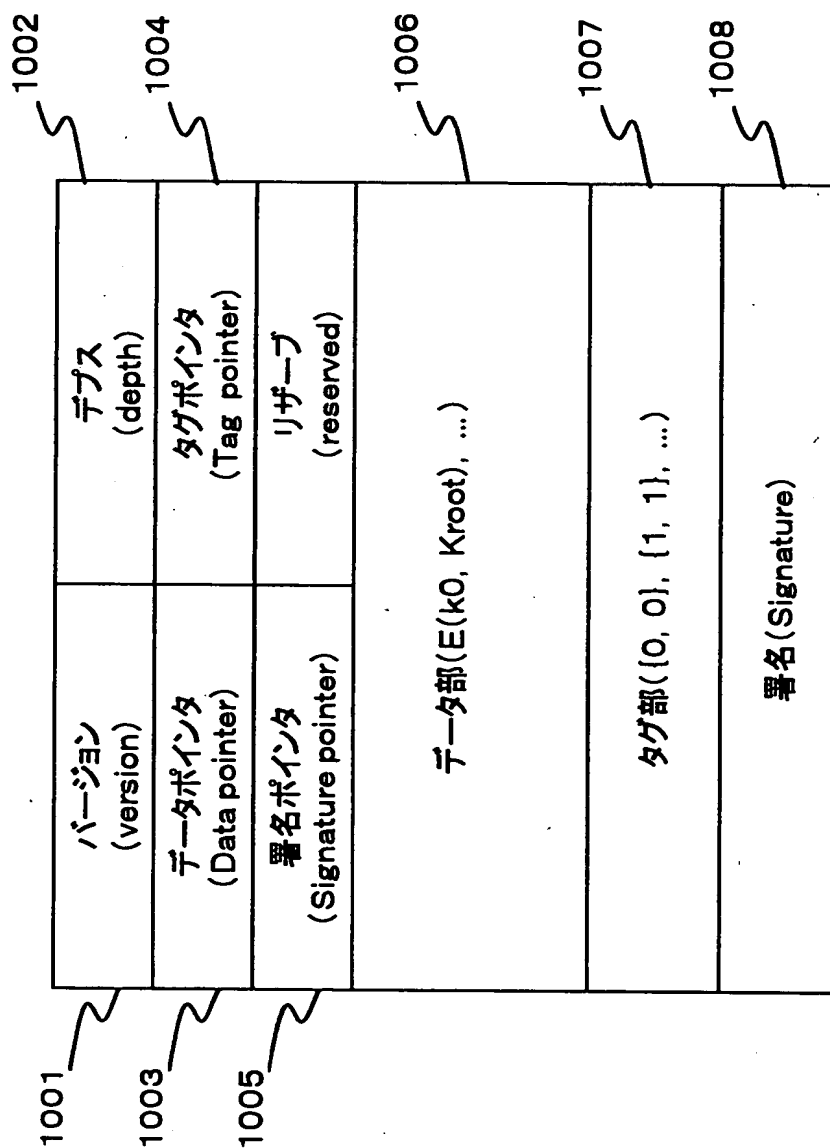
リボケーションリスト

バージョンナンバー
リボーク機器ID
:
センタのデジタル署名

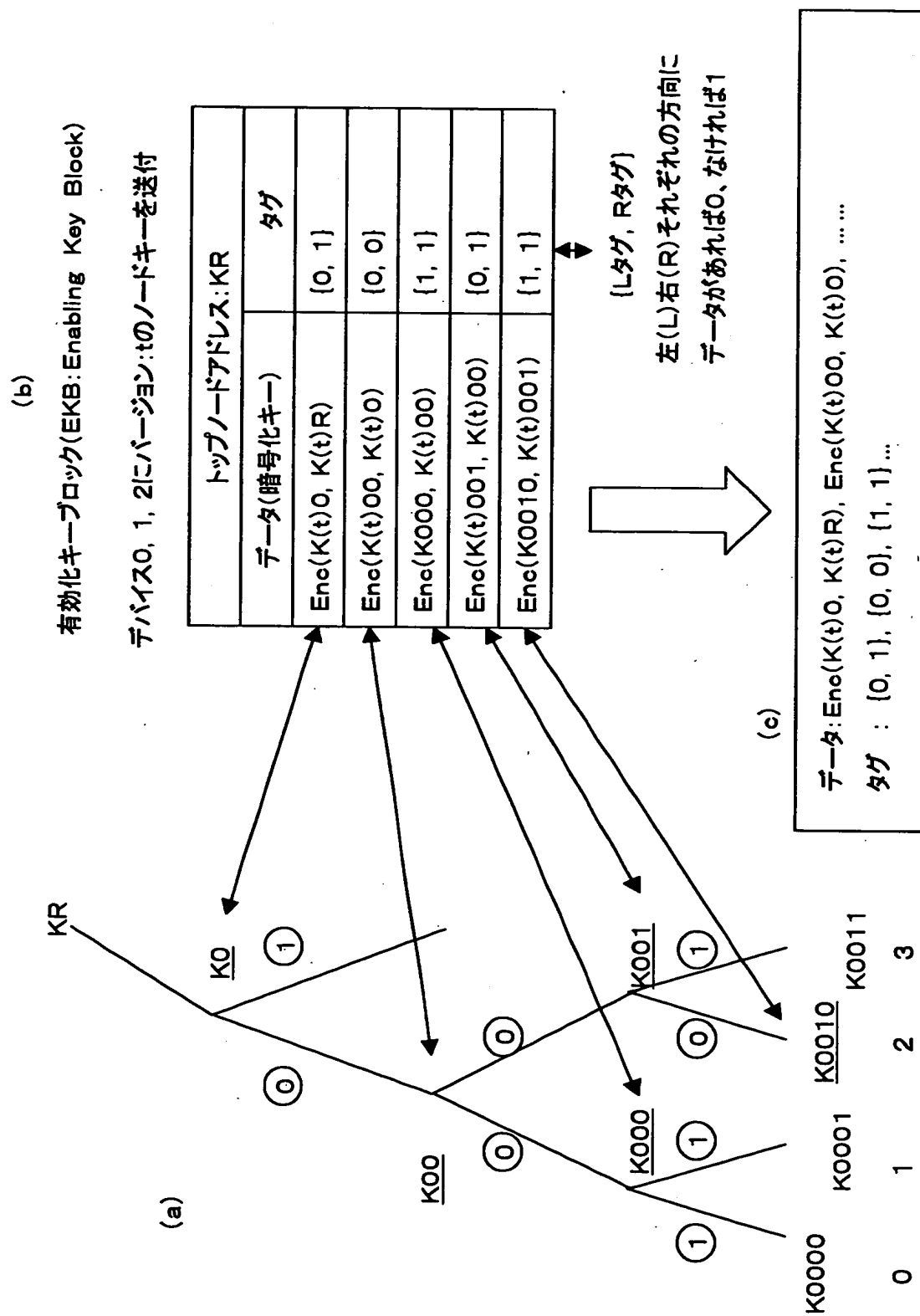
【図 24】



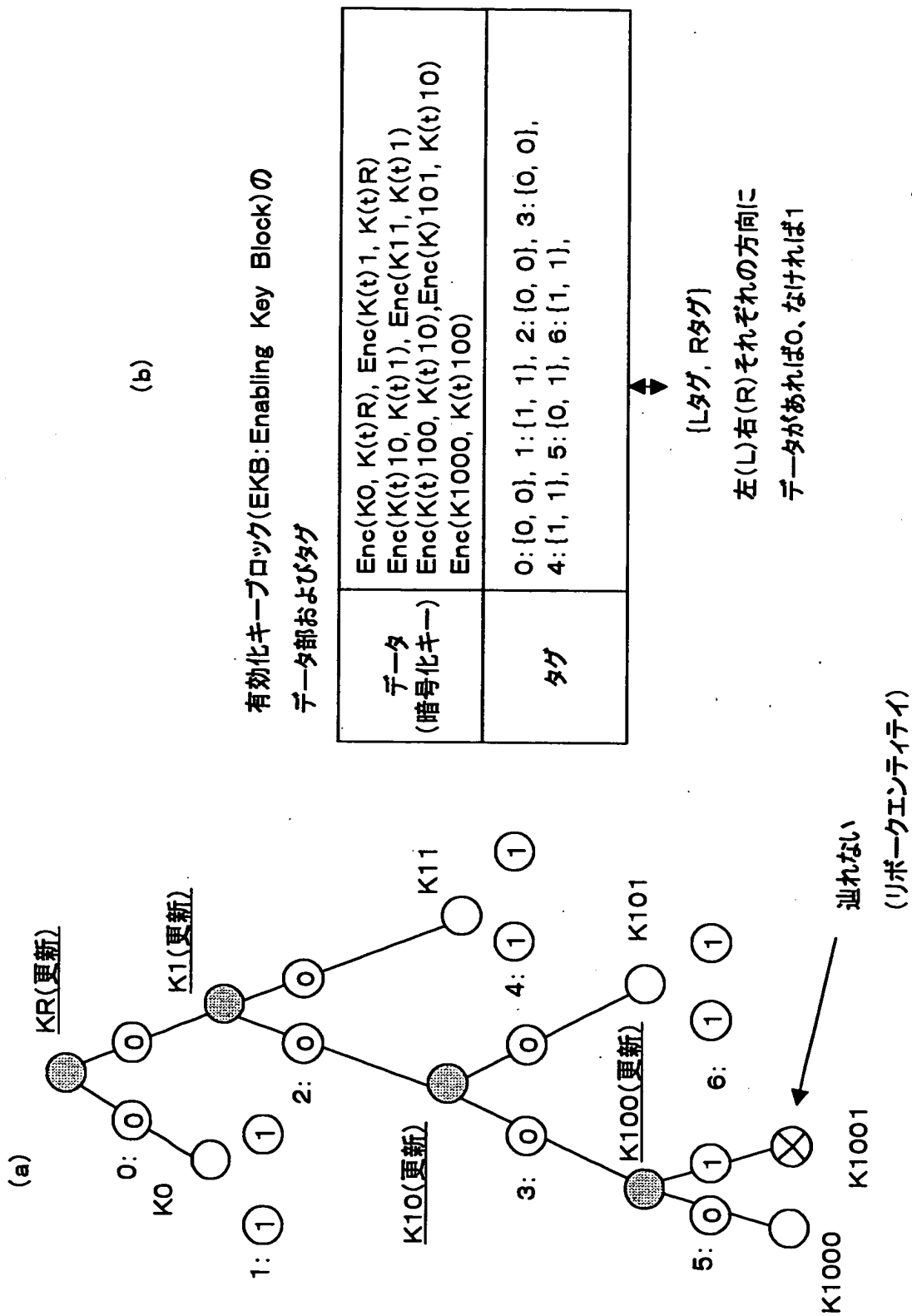
【図 2 5】



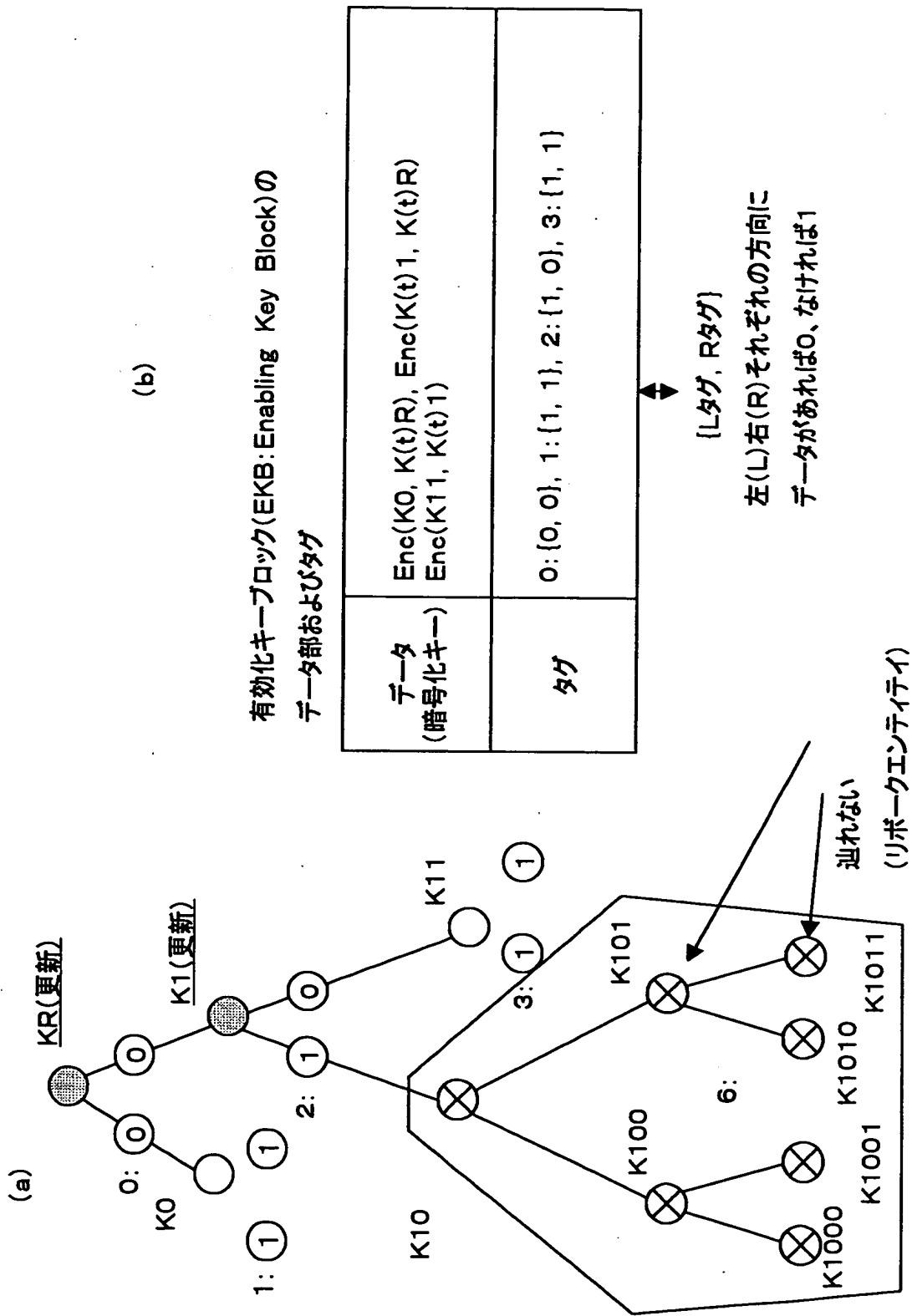
【圖 26】



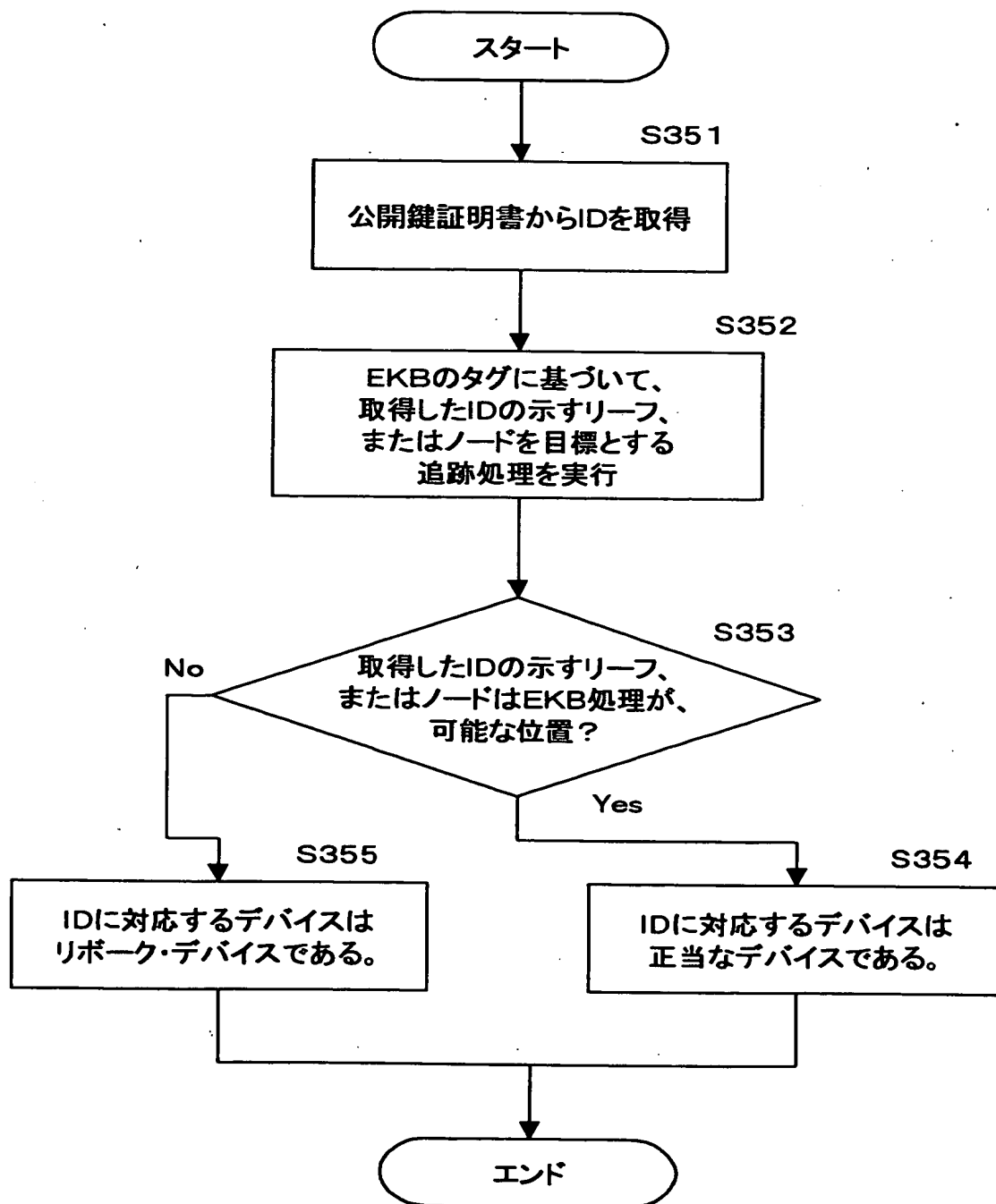
【図 27】



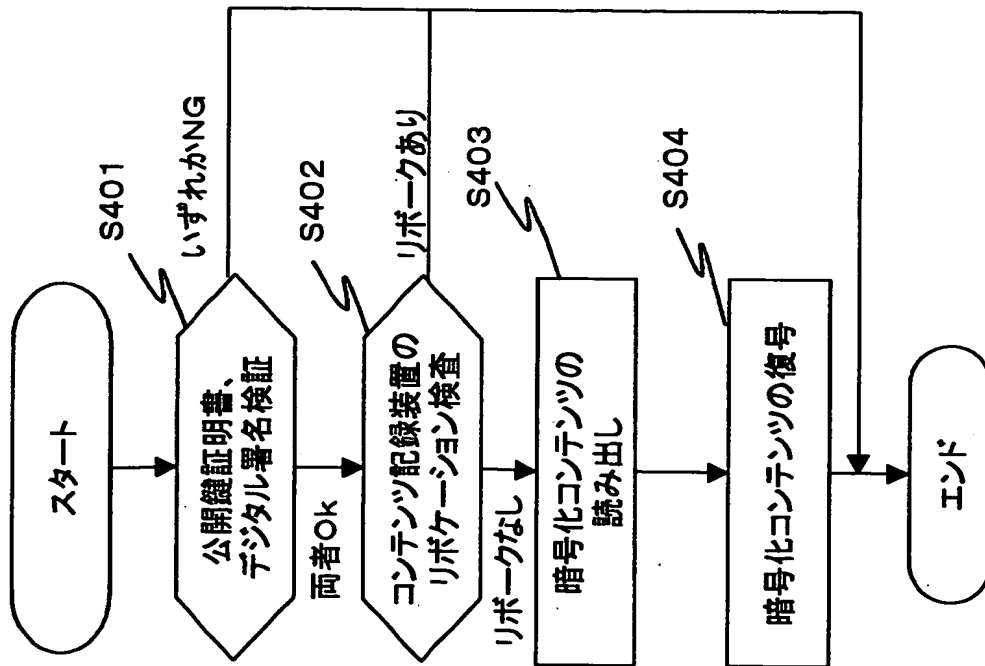
【図28】



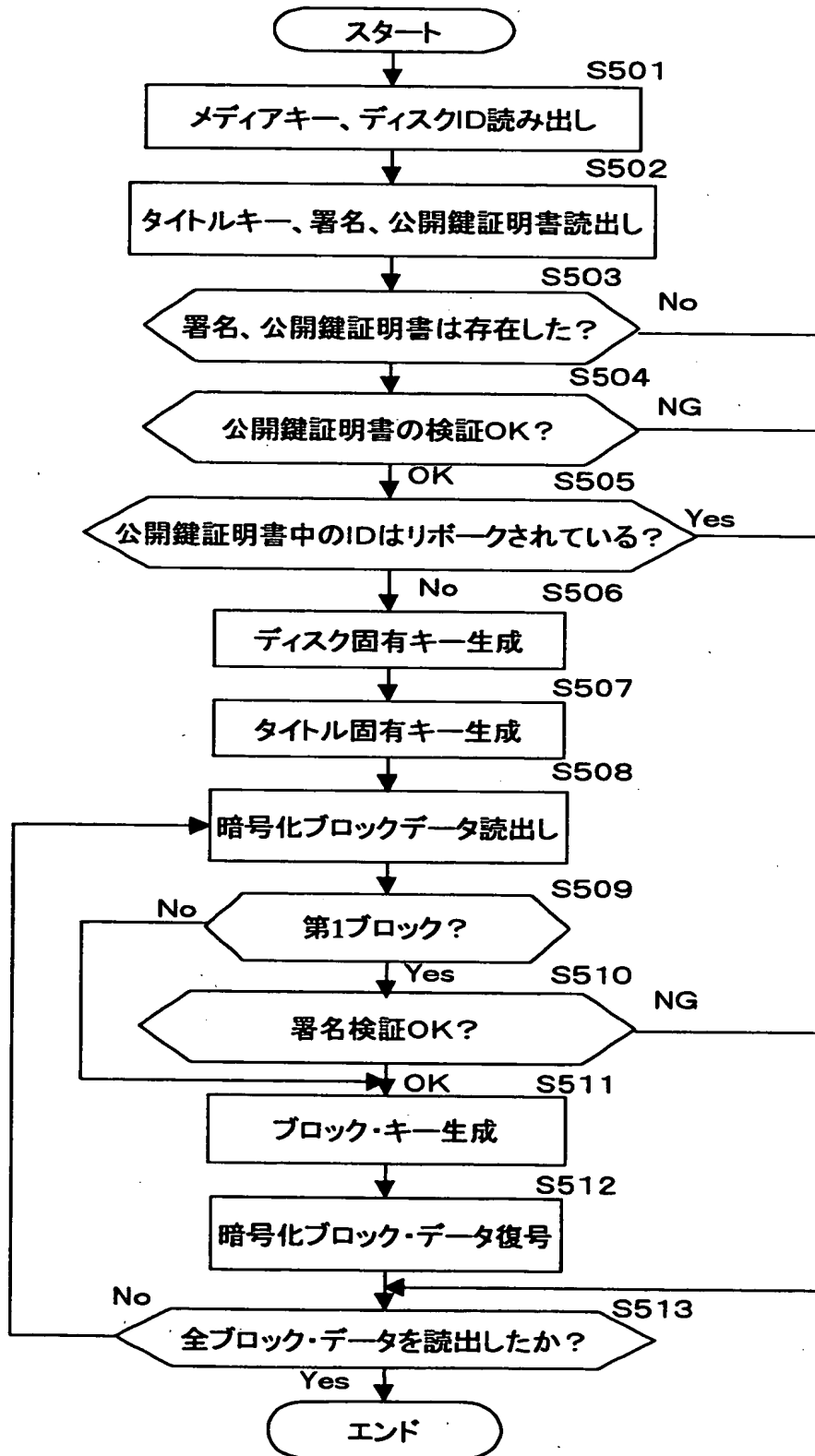
【図 29】



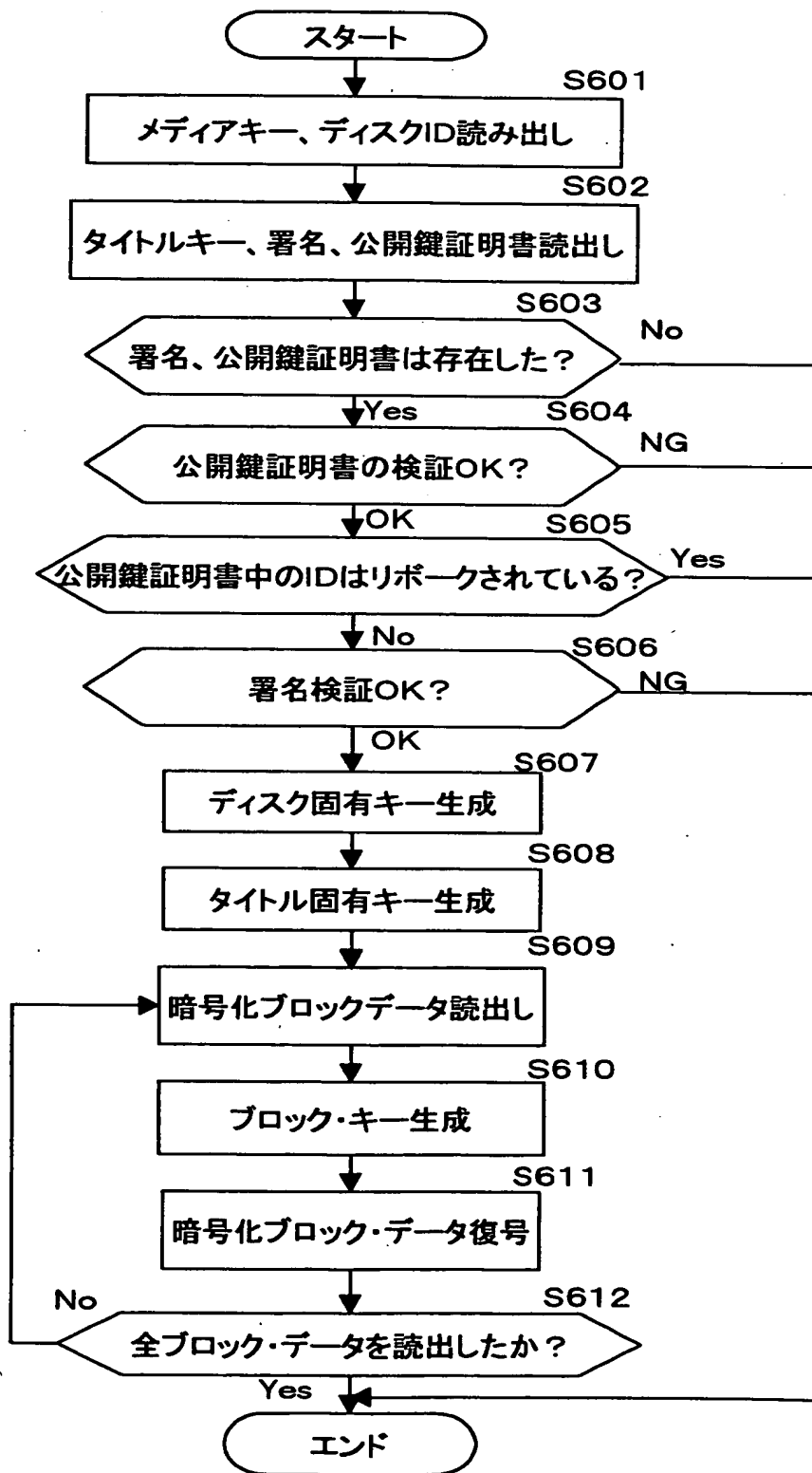
【図30】



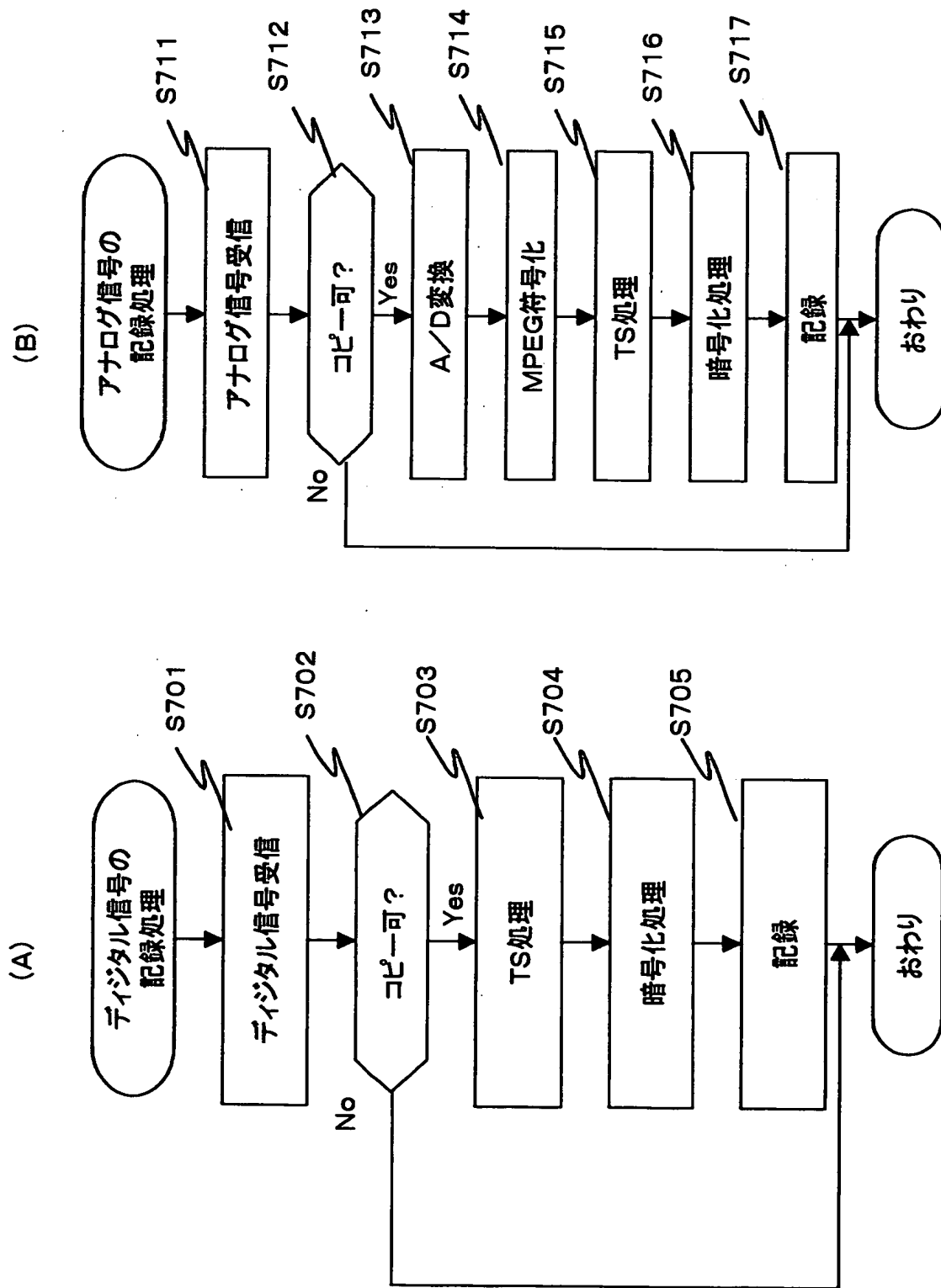
【図 31】



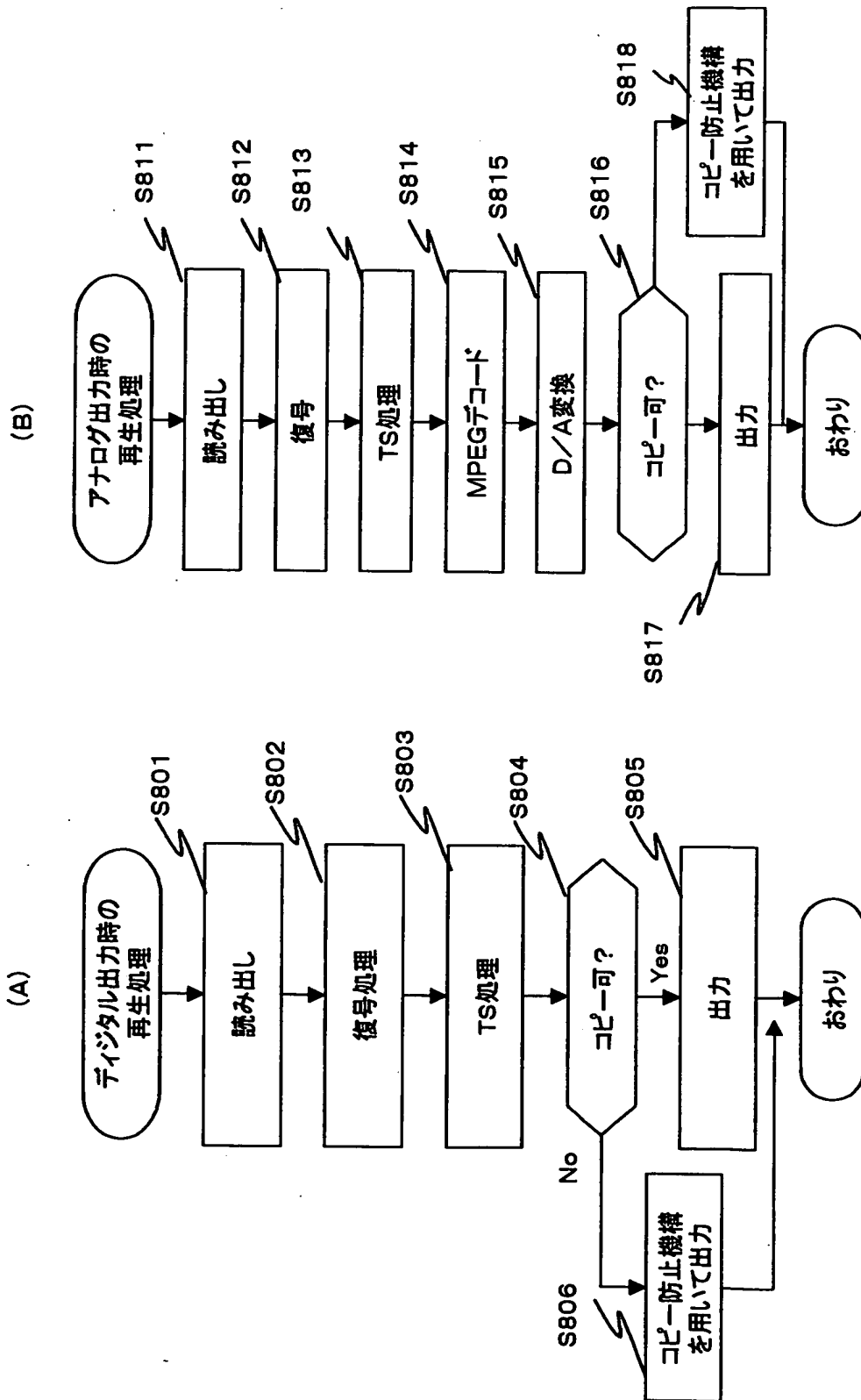
【図 32】



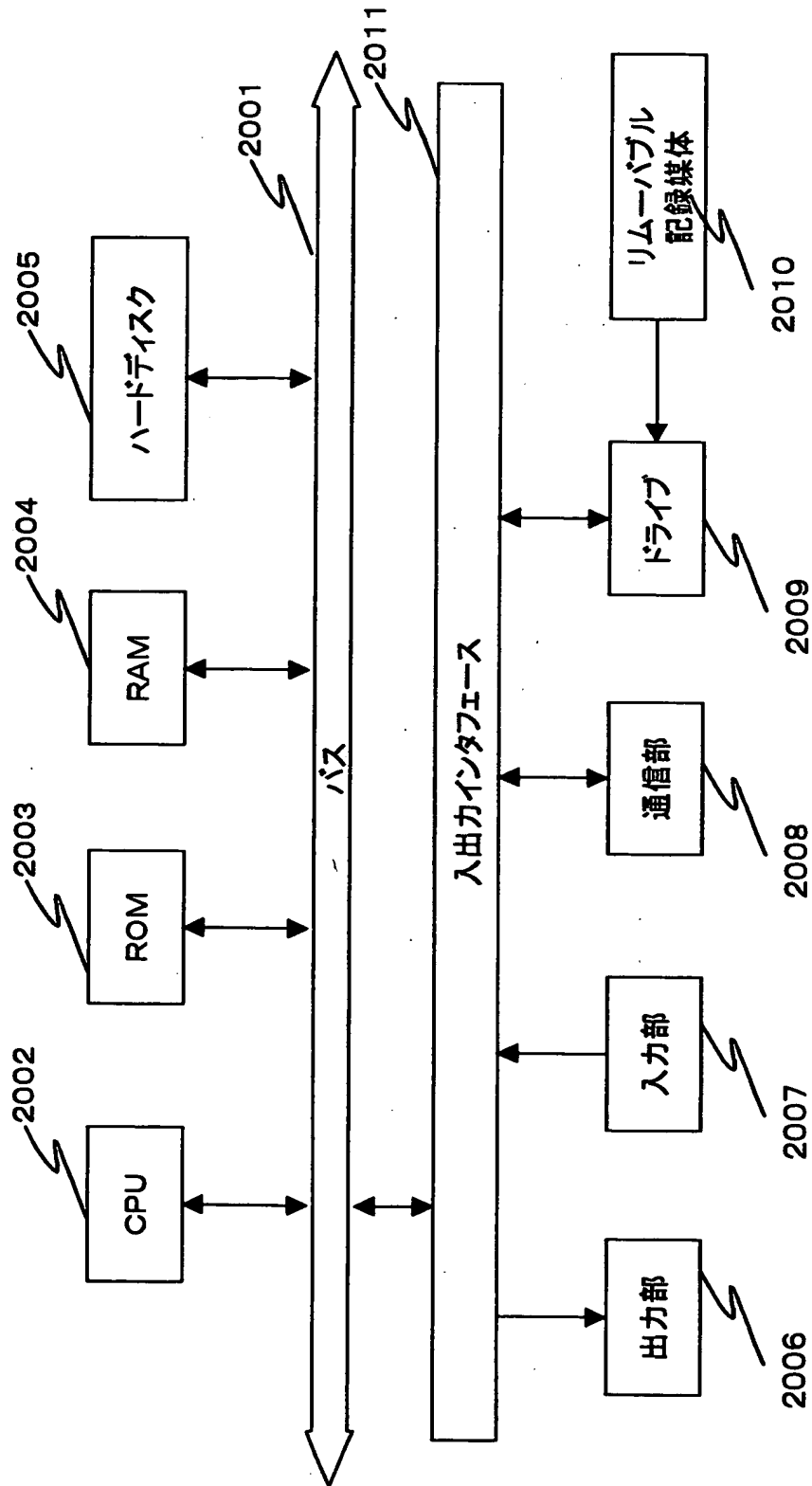
【図 33】



【図 34】



【図 35】



【書類名】 要約書

【要約】

【課題】 コンテンツ再生において、正当な記録コンテンツ記録であるか否かを判定して再生する構成を持つ情報記録再生装置および方法を提供する。

【解決手段】 データを情報記録媒体に記録する際にデジタル署名および公開鍵証明書を記録し、コンテンツを記録した記録装置を特定可能とした。不正に記録されたデータを含む記録媒体が流通しても、記録装置を特定しシステムからの排除が行える。情報再生装置は、データを読み出す際に署名および公開鍵証明書の正当性を確認し、コンテンツ記録者を特定し、公開鍵証明書、デジタル署名の改竄の無いことを確認した後にデータを再生する。本構成により、不正な記録装置による記録コンテンツの利用（再生）の効率的排除が可能となる。

【選択図】 図 3 1

出 願 人 履 歴 情 報

識別番号 [000002185]

1. 変更年月日 1990年 8月30日

[変更理由] 新規登録

住 所 東京都品川区北品川6丁目7番35号

氏 名 ソニー株式会社